DOI 10.36622/VSTU.2023.4.26.004
УДК 004.056.47

ИНФОРМАЦИОННАЯ КАРТА КИБЕРКОНФЛИКТА «ПАЛЕСТИНА-ИЗРАИЛЬ»

А.Л. Сердечный, А.Г. Остапенко

Процессы информационного противоборства в киберпространстве тесно связаны с глобальной политической обстановкой. Риски компьютерных атак на государственные, промышленные, финансовые и частные информационные системы возрастают с обострением конфликтов между государствами в том числе в результате активизации политически мотивированных хакеров (хактивистов). За последние годы данный источник угроз превратился в хорошо организованную силу, способную проводить сложные и долговременные операции, действуя совместно с киберпреступниками и APT-группировками. В настоящей статье представлены результаты исследования киберконфликта «Палестина-Израиль», которое направлено на выявление скрытых связей между субъектами рассматриваемого конфликта. Исследование проводилось с помощью метода информационного картографирования, позволившего структурировать сведения от более чем 150 группировок хактивистов из стран Арабского и Индо-Тихоокеанского регионов. В результате информационно-картографического анализа были получены оценки обстановки, сложившейся в киберпространстве рассматриваемых регионов, а также сформирован набор данных о деятельности соответствующих хактивистких группировок за период с 6 октября по 11 ноября 2023 года.

Ключевые слова: хактивисты, информационная карта, кибервойна, Палестина-Израиль.

Введение

Конфликты в киберпростарнстве существенным образом зависят от глобальной военной, экономической и политической обстановки. Их протекание осуществлять в нескольких «плоскостях»:

- борьба хактивистов с государствами и сетевыми организациями, как один из аспектов разрешения трехстороннего противоречия между государствами, транснациональными корпорациями и свободной личностью;
- деятельность фанансово-мотивированных группировок;
- разведывательная деятельность APT-группировок.

Во время обострения обстановки данные «плоскости» часто пересекаться, а субъекты могут проявлять признаки как хактивистов и финансово-мотивированных хакеров, так и высокоорганизованных APT-группировок. Появляются альянсы и ситуационные взаимодействия между различными коллективами, которые в последствии могут перерасти в профессиональные киберсилы, способные долгосрочно организовывать свою деятельность и проводить сложные скоординированные операции в киберпространстве.

Риски компьютерных атак на государственные, промышленные, финансовые и частные информационные системы возрастают с возникновением военных конфликтов. На первый план выходят политически мотивированные хакеры [1-2]. За последние годы данный источник угроз вышел на первый план и по уровню ущерба стал заметен по сравнению с киберпреступностью, а по сложности организации сопоставим с некоторыми APT-группировками.

В настоящее время научный интерес вызывает киберконфликт между Палестиной и Израилем, который в киберпространстве не ограничивается лишь данными участниками, а охват несколько регионов. Проведённое исследование было направлено на выявление скрытых связей между субъектами рассматриваемого конфликта. Оно дополняет ранее полученные результаты изучения киберпространства [3-6].

Субъектами противостояния в информационном пространстве являются более 150 группировок хактивистов, которые можно отнести к глобальным сетевым сообществам, конкретным странам или языковым и культурным группа Арабского и Индо-Тихоокеанского регионов.

При этом необходимо отметить, что в рамках исследования определение принадлежности группировки к той или иной стране, языковой или культурной группе определялась на основании как косвенных признаков, проявляемых через публикуемые сообщения группировок в социальной платформе Telegram, так и свидетельств, публикуемых самими группами на своих информационных ресурсах. Подлинность и неизменность сообщений невозможно подтвердить ввиду технических особенностей работы социальной платформы, так как сообщения могут быть изменены авторами соответствующих каналов или чатов, а сами авторы являются анонимными источниками.

В связи с этим использование в настоящей статье меток с названиями стран в отношении хактивистов осуществляется для связи процессов, происходящих в киберпространстве, с процессами в реальном мире. **Такие метки нельзя рассматривать как объективные факты принадлежности группы хактивистов соответствующей стране, языковой или культурной группе**.

По теме исследований имеется ряд публикаций [7-13] от экспертов, занимающихся мониторингом и изучением процессов, происходящих в киберпространстве. Наиболее полными в плане рассмотрения сторон конфликта являются работы [7-9] австралийского исследователя с псевдонимом CyberKnow, а также сотрудников компаний Tsanct Technologies и Würth Phoenix. В их публикациях приводится состав групп, указывается принадлежность к одной из сторон конфликта, отмечается специализация группировок, а также рассматривается аналитика некоторых инцидентов, о которых стало известно в результате появления сообщений от хактивистов.

В работе австралийского автора CyberKnow [7], датируемой 2 ноября 2023 года, приводится перечень из 137 группировок, 19 из которых выступают на стороне Израиля, а 128 – Палестины. Исследователь одним из первых начал вести хронологию инцидентов кибервойны. Каждый день в его микроблоге размещаются новости от хактивистов и других источников атак на государственные системы различных стран. Наиболее известной работой CyberKnow является КиберТрэкер (CyberTracker) киберконфликта «Россия-Украина», представляющий собой карту группировок, участвующих в соответствующем противостоянии. Карта периодически обновляется и публикуется на его информационных ресурсах. Работа [7] является аналогом этого проекта, но в отношении Палестино-Израильского киберконфликта. CyberKnow отмечает, что по количеству участников конфликт превзошёл Российско-Украинский.

В работе [8], которая вышла 18 октября 2023 года, которую разместили сотрудники компании Tsanct Technologies на своём информационном ресурсе FalconFeeds, представлены сведения о 113 группировках. Названия некоторых группировок из обоих перечней различаются. Также важным источником является репозиторий [9] Массимо Джаймо (Massimo Giaimo) из Würth Phoenix, в котором он приводит ссылки на Telegram-каналы группировок, обнаруженные в результате поиска названий хактивистов из отчёта [8]. При этом некоторые группы найдены не были (например, хактивисты AnonyMiss).

Главным ограничением рассмотренных работ является то, что в них не указываются отношения между группировками, что ввиду их большого количества затрудняет анализ процессов, происходящих в рамках рассматриваемого киберконфликта. Несмотря на то, что результаты исследований авторов [7, 8] сведены на географической карте, локализация групп сосредоточена только лишь в области Палестины или Израиля и не отражает связь субъектов с реальными процессами, которые послужили причиной участия той или иной группировки в конфликте. Кроме того, в работе [6] было показано, что в киберпространстве понятие физических границ размыто и не всегда

отражает суть информационных процессов, поэтому их изображение с использованием географических карт не обеспечивает наглядное представление ключевых взаимосвязей между субъектами, объектами и процессами, что в итоге не способствует лучшему пониманию обстановки.

Для преодоления указанного ограничения может быть использована информационная карта, построенная на основе исходных данных, отражающих взаимосвязи между субъектами как в физическом, так и в информационном и социальном слоях киберпространства [6].

Алгоритм исследования

Исследования проводились с помощью информационно-картографического метода, изложенного в монографии [6]. Алгоритм исследований показан на рис. 1.

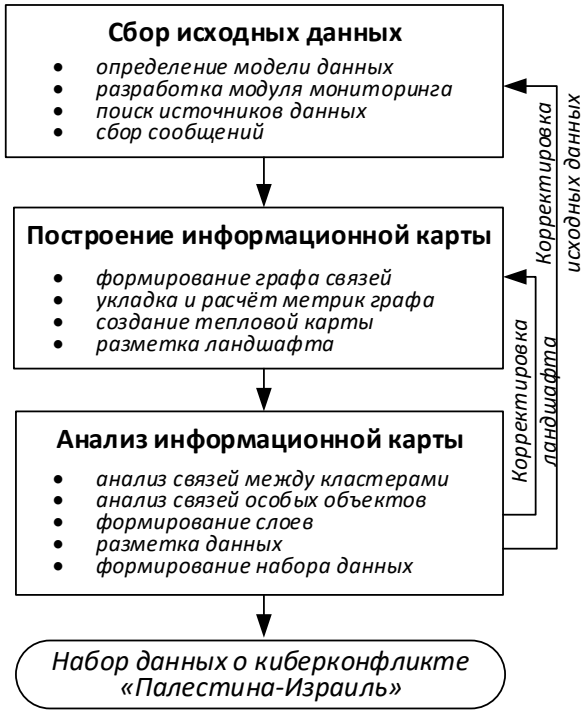

Рис.1. Алгоритм исследования киберконфликта «Палестина-Израиль»

В ходе анализа источников [7-13] было установлено, что подавляющее большинство стороны киберконфликта «Палестина-Израиль» в качестве информационной площадки используют социальную платформу Telegram. Для сбора сведений с данной платформы использован модуль, разработанный в рамках проекта «Безопасный интернет» [5], который положительно зарекомендовал себя при решении схожих задач.

Модель данных включала следующие сущности:

- «Telegram-канал или чат»;
- «сообщение из Telegram-канала или чата»;
- «Текст сообщения»;
-«Файл, прикреплённый к сообщению»;
- «Фотография, прикреплённая к сообщению»;
- «Видео, прикреплённое к сообщению»;
- «Аудиофайл, прикреплённый к сообщению»;
- «Гиперссылка, содержащаяся в тексте сообщения».

Модель данных была дополнена сущностью «Хактивисткая группировка» и связью с сущностью «Хактивисткая группировка».

В качестве источников исходных данных выступали Telegram-каналы, сведения о которых были найдены в открытых источника [7-13]. Поиск проводился как с использованием штатных возможностей социальной платформы Telegram, так и в результате анализа предварительных ландшафтов информационной карты, позволявшего выявлять Telegram-каналы и чаты по репостам сообщений из тематически близких каналов.

Во время формирования перечня источников было установлено, что в [7-9] имеются дублирования группировок (например, у CyberKnow [7] группировки Pakistani Leet Hackers, STUCX TEAM, C.O.A member и Esteem Restoration Eagle упоминаются дважды, а в [9] дублируются Termux Israel, Cyber Club, AnonTI3x Group, YourAnon T13x; KEP TEAM).

Помимо Telegrom-каналов хактивистов, отмеченных в работах [7-13], в качестве источников данных также рассматривались Telegram-каналы, которые больше всего утомились в найденных источниках и являлись информационной площадкой хактивистов, которые занимали нейтральную

группировками. Всего было собрано более 400 тыс. сообщений. Половина из них

публиковалась в период с 6 октября по 11 ноября 2023 года в каналах 152 группировок хактивистов – сторон киберконфликта.

Для построения ландшафта информационной карты был сформирован и уложен (с помощью силового алгоритма понижения размерности ForceAtlas2) граф свей Telegram-каналов или чатов с публикуемыми сообщениями и соответствующими хативисткаими группами, которым они принадлежат. Описание информационной карты приведено в табл. 1. Размеченный ландшафт представлен в виде тепловой карты (рис. 2). Создание слоёв осуществлялось путём нанесения в виде условных изображений на ландшафт информационной карты дополнительных отметок, показывающих исследуемые свойства объектов. Так, например, на рис. 3 показан слой карты с группировками хактивистов, являющихся сторонами конфликта. Группы хактивистов, принимающих ту или иную сторону, показаны пиктограммами в виде соответствующего флага.

Информационная карта «Субъекты киберконфликта «Палестина-Израиль» в социальной платформе Telegram»

Ландшафт информационной карты представлены в виде кластеров (на рис. 2 – областей серого цвета), в которые группируются наиболее связанные Telegram-каналы и чаты участников киберконфликта «Палестина-Израиль». Расположение и расстояние между кластерами отражает близость отношений между хактивисткими группировками. Наиболее близкие кластеры более связаны друг с другом сильнее, чем с кластерами из разных областей карты.

Это свойство позволяет выявлять скрытые взаимосвязи между субъектами в результате анализа состава и расположения объектов, составляющих кластеры. Так, например, если какая-либо группировка в описаниях своих Telegram-каналов или размещаемых сообщениях явно не указывала свою принадлежность к какому-либо хакерскому сообществу, но при этом цитирует и цитируется другими каналами, входящими в тот же кластер, то можно предположить, что такая группировка состоит в дружеских отношениях с хактивитами кластера и обладает некоторыми схожими свойствами (общностью целей или принадлежностью своих членов к определённой стране или организации). Данный тезис применим и к группе кластеров, для которой может наблюдаться сходство по признакам принадлежности к географическому региону, стороне конфликта, языковой или этнической группе, роду занятий.

На рис. 2 пунктирными линиями показаны четыре основные группы кластеров, образующих ландшафт карты:

- «хактивисты Индо-Тихоокеанского региона»;
- «хактивисты Арабского региона»;
- «хактивисты, связанные с киберпреступностью»;
- «хактивисты, связанные с Израилем и Ираном».

Данные группы кластеров фокусируют внимание на основных зонах киберконфликта.

Интересной особенностью, которую нельзя установить по изображениям на географических картах от Cyberknow [7] и Tsanct Technologies [8] является то, что большая часть группировок киберконфликта «Палестина-Израиль» сосредоточена в странах Индо-Тихоокеанского региона, где в киберпространстве одновременно с рассматриваемым конфликтом ведется борьба хактивистов Индии и азиатских стран, в которых достаточно большая доля мусульманского населения.

Данная особенность определяет расположений кластеров в нижней части информационной карты. Кластеры хактивистов из Индонезии, Малайзии, Пакистана, Бангладеша, переплетены между

Таблица 1

Сведения об информационной карте «Субъекты киберконфликта «Палестина-Израиль» в социальной платформе Telegram»

Тип сведений	Характеристика информационной карты
Задачи, решаемые с помощью карты	Систематизация сведений о силах киберконфликта «Палестина-Израиль»; выявление скрытых взаимосвязей между хактивисткими группировками, проявленных через объекты атак, цитирование сообщений и лингвистические особенности содержимого таких сообщений; оперативное обнаружение компьютерных атак на защищаемые объекты и инцидентов в результате их успешной реализации; разметка наборов данных для задач обучения искусственного интеллекта
Исходные данные	Сообщения от хактивистких группировок Арабского и Индо-Тихоокеанского регионов, опубликованные в социальной платформе Telegram в период с 6 октября по 11 ноября 2023 года
Модель данных	*Узлы*: (t) – «Telegram-канал или чат»; (m) – «сообщение из Telegram-канала или чата»; (txt) – «текст сообщения из Telegram-канала или чата»; (tag) – «тэг из текста сообщения»; (f) – «файл, прикреплённый к сообщению»; (p) – «фотография, прикреплённая к сообщению»; (v) – «видео, прикреплённое к сообщению»; (a) – «аудиофайл, прикреплённый к сообщению; (u) – «гиперссылка, содержащаяся в тексте сообщения»; (act) – «хактивисткая группировка» *Связи*: [part1]: (t)←(m) – «Публикация сообщения в канале»; [repost]: (m)←(t) – «Репост сообщения из канала»; [in]: (m)←(m) – «Связь между сообщениями (для сообщений из чатов и репостов); [part2]: (m)←(tag) – «Тэг в сообщении»; [part3]: (m)←(f) – «Файл в сообщении»; [part4]: (m)←(txt) – «Текст в сообщении»; [part5]: (m)←(p) – «Фотография в сообщении»; [part6]: (m)←(v) – «Видео в сообщении»; [part7]: (m)←(u) – «Гиперссылка в сообщении»; [part8]: (m)←(a) – «Аудио в сообщении»; [rel]: (act) ⇄ (act) – «Группировки связаны, но тип связи не определён»; [eq1]: (act) ⇄ (act) – «Установлена идентичность двух группировок, которые ранее рассматривались как разные»; [part9]: (act) ← (act) – «Группировка является частью другой»; [next]: (act) ← (act) – «Преемственность группировок»; [eq2]: (act) ⇄ (t) – «Telegram-канал или чат ведется группировкой» *Свойства*: «Уникальный идентификатор»: для объектов (t), (m), (txt), (f), (p), (v), (a), (u), (act); «Название»: для объектов (t), (f), (p), (v), (a), (act); «Описание/Текст»: для объектов (t), (txt) и (act); «Дата публикации», «Дата модификации», «Количество просмотров», «Количество репостов»: для объекта (m); «Ссылка на источник»: для объекта (u); «Логотип»: для объектов (t) и (act); «Сторона конфликта»: для объекта (act)
Процедура построения карты	В ходе построения карты осуществлены следующие операции: - автоматический сбор и внесение в СУБД Neo4j сведений из 383 Telegram-каналов (чатов; - построение графа связей [part1], [repost], [eq2], [part9], [rel]; - укладка графа в двухмерном пространстве с помощью силового алгоритма ForceAtlas2 (LinLog = true, «Влияние весов рёбер» = 1, «Запрет перекрытия» = true, «Устойчивость» = 1, Theta = 1.2, «Разрежённость» = 10, «Гравитация» = 1); - построение тепловой карты на основании графа связей («Радиус»=0.015, «Распределение пикселей»=0,001); - автоматизированная разметка кластеров хактивистких группировок; - формирование слоёв информационной карты для анализа связей между хактивистами
Ландшафт	Разметка ландшафта отражает наименование кластеров хактивистких группировок, которые присваивались экспертом исходя из сходства групп, находящихся в одной области
Слои	«Стороны киберконфликта «Палестина-Израиль», «Индийские хактивисты», «Индонезийские хактивисты», «Малазийские хактивисты», «Хактивисты Пакистана, Бангладеша, Марокко и Йемена», «Мусульманские хактивисты», «Хактивисты, связанные с Израилем, Турцией и Ираном», «Глобальные сообщества хактивистов и киберпреступников»
Форматы карты	.html (карта для выгрузки на сайт), .qgz (карта для программы QGIS), .gephi (графы для программы Gephi), .zip (дамп базы данных Neo4j)

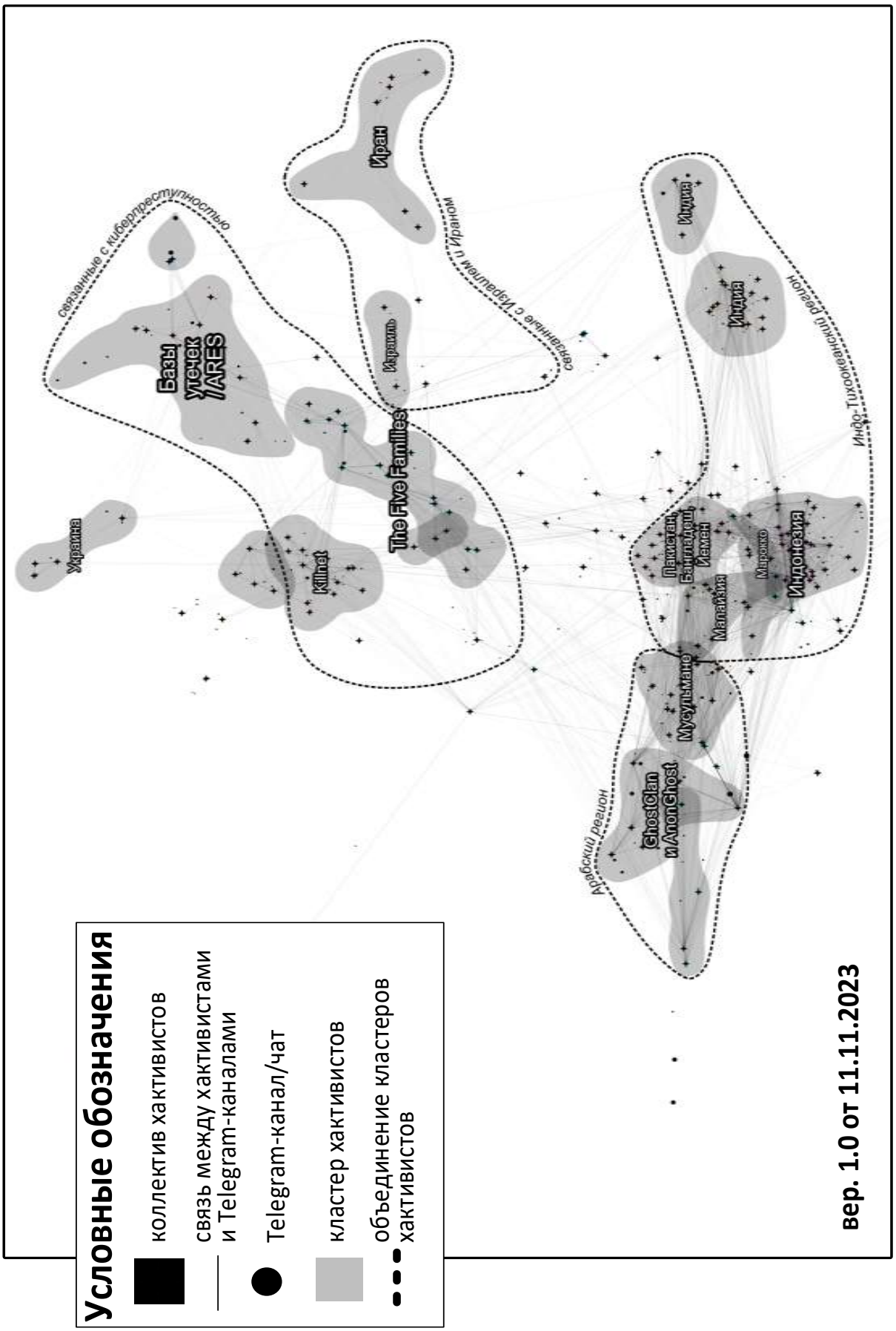

Рис. 2. Информационная карта «Субъекты киберконфликта «Палестина-Израиль» в социальной платформе Telegram»

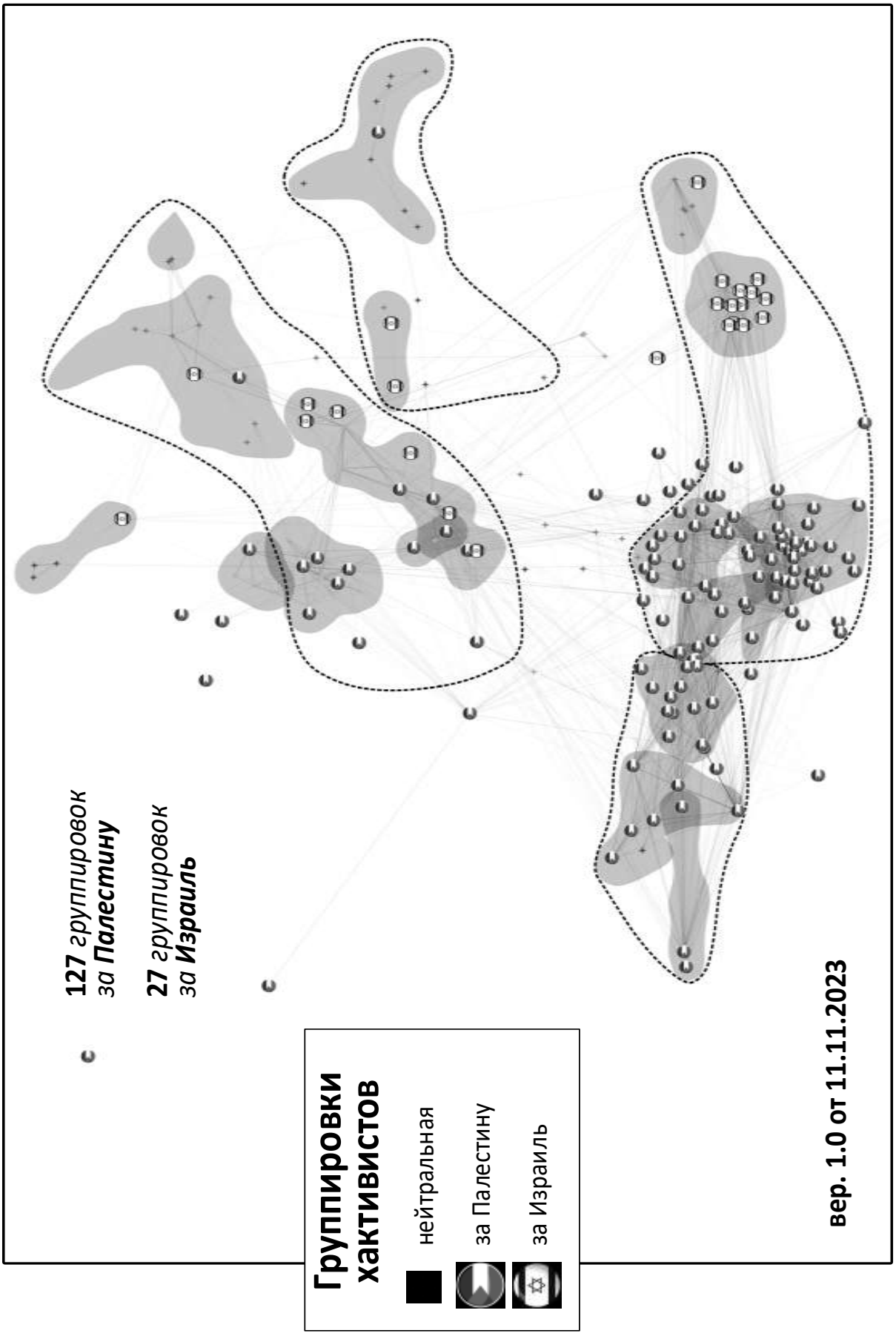

Рис. 3. Изображение на информационной карте сторон киберконфликта «Палестина-Израиль»

собой и расположены ближе к мусульманскому кластеру, чем к кластеру хактивистов из Индии, несмотря на географическое положение стран, интересы которых выражают хакерские сообщества.

На рис. 4 показан кластер «Индийские хактивисты», который разделён на две части. В левой части расположены хактивисты, связанные с киберармией Индии. Они в полном составе поддерживают Израиль и наиболее активны среди произраильских группировок. Indian Cyber Force была одной из первых, кто объявил о начале кибератак на Палестину [8].

В правой части только группировка SilentOne поддержала Израиль, остальные – в нейтральном статусе. Индийские группировки в своих сообщениях используют хэштэги с названием групп, участвующих в атаке. Хэштэг с названием цели или кампании (например, #OppPk – операция против Пакистана) используется редко. По динамике публикации сообщений, показной на графике (рис. 5) можно наблюдать спад активности Индийских хактивистов.

Против Индии проводят атаки группировки из Индонезии, Малайзии, Пакистана, Бангладеша. Наиболее многочисленными являются кластеры Индонезии (рис. 5) и Малайзии (рис. 6).

Основная деятельность групп в публичном пространстве сводится к организации DDoS-атак на объекты Израиля и Индии, взлом и дейфейс сайтов, информационно психологическое воздействие на свою аудиторию. Группами активно используются хэштэги с обозначением операций (#FreePalestine, #SavePalestine, #OpIsrael, #OpIndia). Также указываются хэштэги с названием групп, принявших участие той или иной атаке, что позволяет координировать действия, повышает сплочённость коллективов, структурирует информацию об инцидентах и облегчает её поиск с помощью штатных средств социальной платформы Telegram.

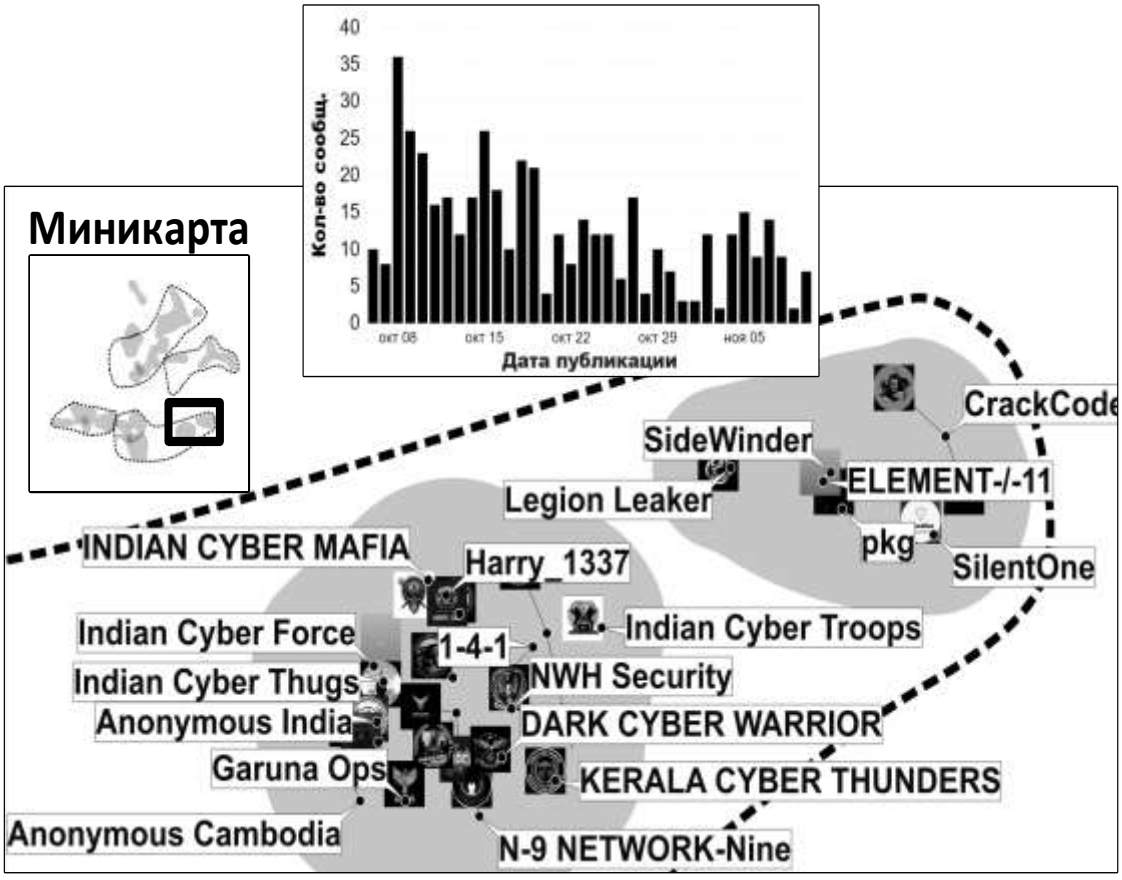

Рис. 4. Индийские хактивисты

Интенсивность сообщений хактивистов Индонезийского кластера остаётся достаточно равномерной на все промежутке наблюдения. Сообщений с хэштэгом #OpIndia примерно в два раза меньше, чем сообщений с хэштэгами #FreePalestine, #SavePalestine, #OpIsrael, но интенсивность подобных сообщений гораздо выше, чем у дружественных хактивистов.

Количество сообщений в Малайзийском кластере пошло на спад после 25 октября (сразу после резкого роста сообщений с хэштэгами западных стран #OpFrance, #OpUSA).

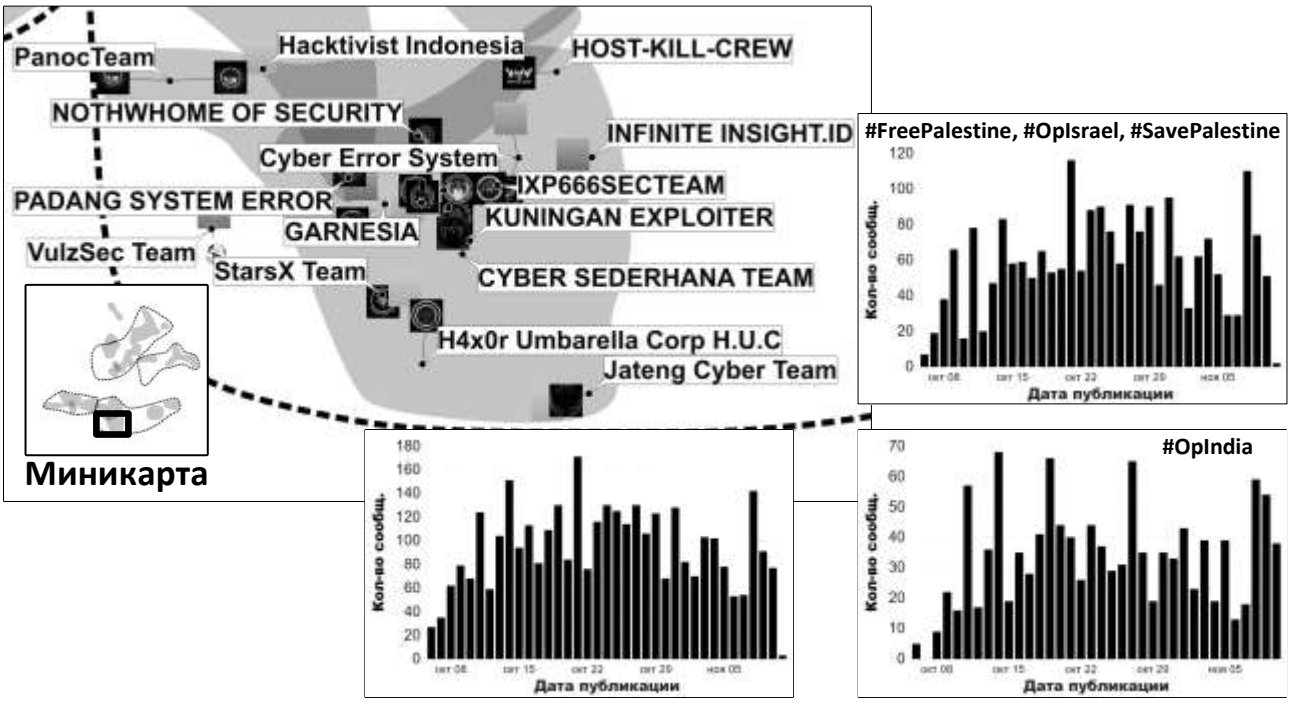

Рис. 5. Индонезийские хактивисты

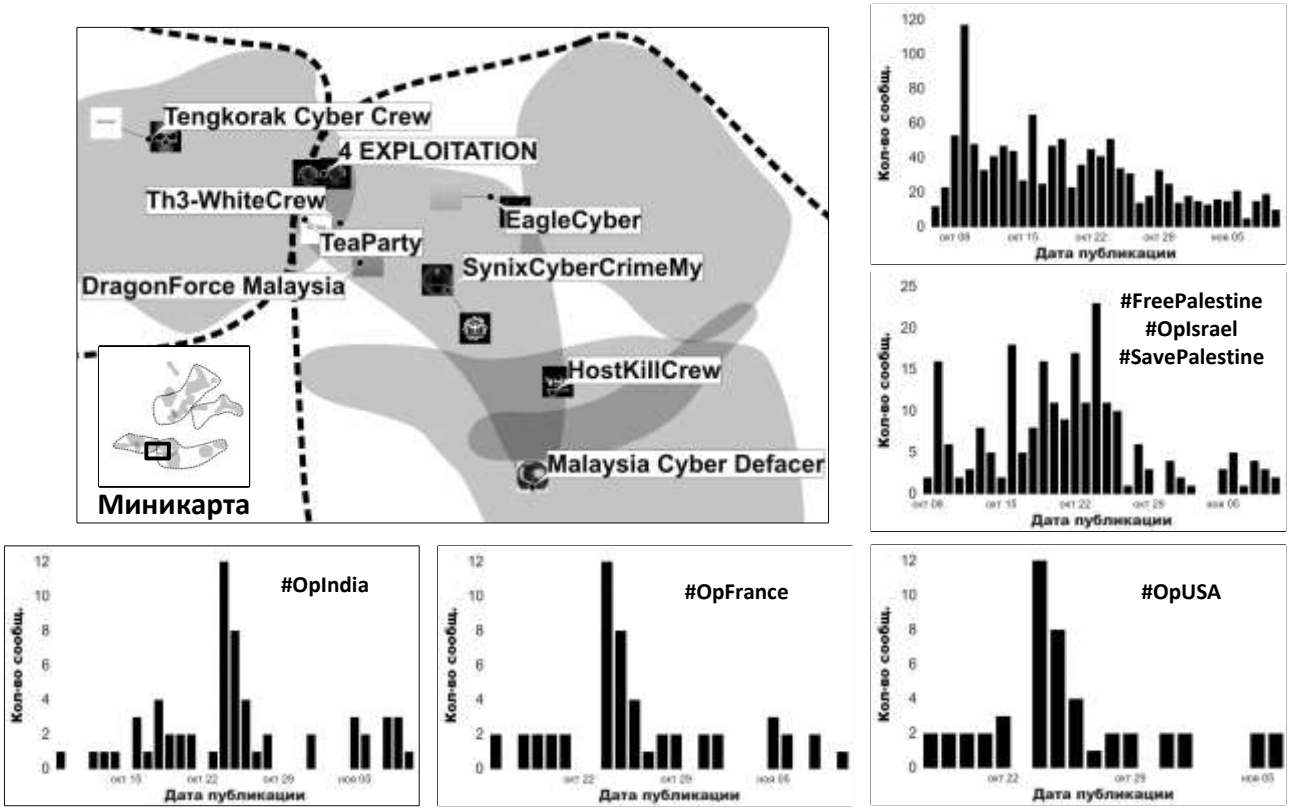

Рис. 6. Малазийские хактивисты

На рис. 7 показаны хактивисты из двух кластеров: «Пакистан, Бангладеш, Йемен» и «Марокко». Наибольшую активность и число группировок демонстрируют хактивисты из Пакистана и Бангладеша. Доля сообщений с хэштегом #OpIndia существенно ниже, чем с хэштегами в поддержку Палестины. У хактивистов Бангладеша заметен хэштэг #OpItaly, а у Пакистана – #OpUSA.

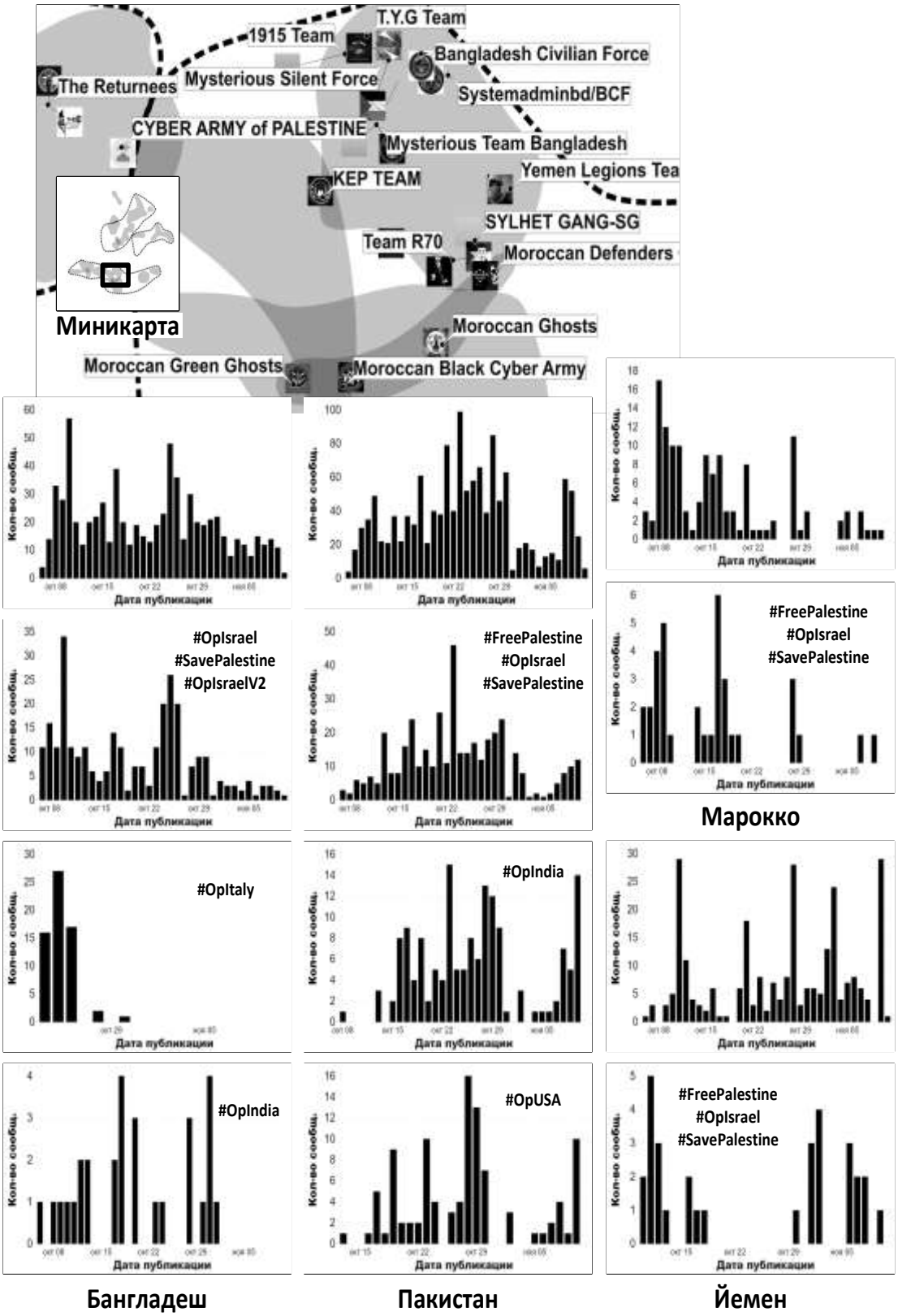

Рис. 7. Хактивисты Пакистана, Бангладеша, Марокко и Йемена

На рис. 8 показаны хактивисты из Мусульманского кластера. Для них наблюдается аналогичная картина. Из особенностей можно отметить большую долю сообщений с вложенными фото и видео материалами.

Таким образом, несмотря на различия в целях, можно сделать вывод, что хактивисты из Арабского и Индо-Тихоокеанского регионов обладают схожим поведением. Они отличаются сплочённостью, что проявляется в большой связанности Telegram-каналов, а использовании группами хэштэгов с названиями коллективов, которые участвовали в скоординированной атаке. Список таких хэштэгов в одном сообщении по объёму может превышать информационную часть сообщения. Сами атаки имеют больше медийное значение, чем наносят реальный ущерб.

Центральное место в киберконфликте «Палестина-Израиль» занимают группировки Ирана и Израиля (рис. 9). Их атаки на критическую информационную инфраструктуру и важные государственные информационные системы несут наибольшие риски.

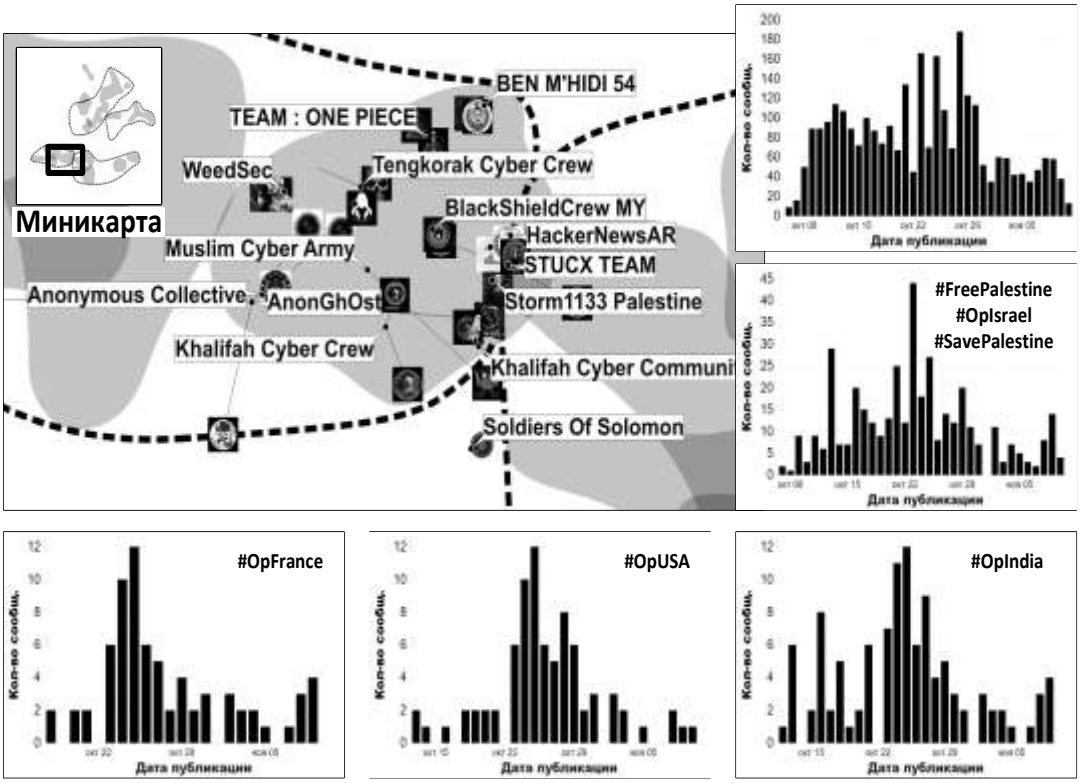

Рис. 8. Мусульманские хактивисты

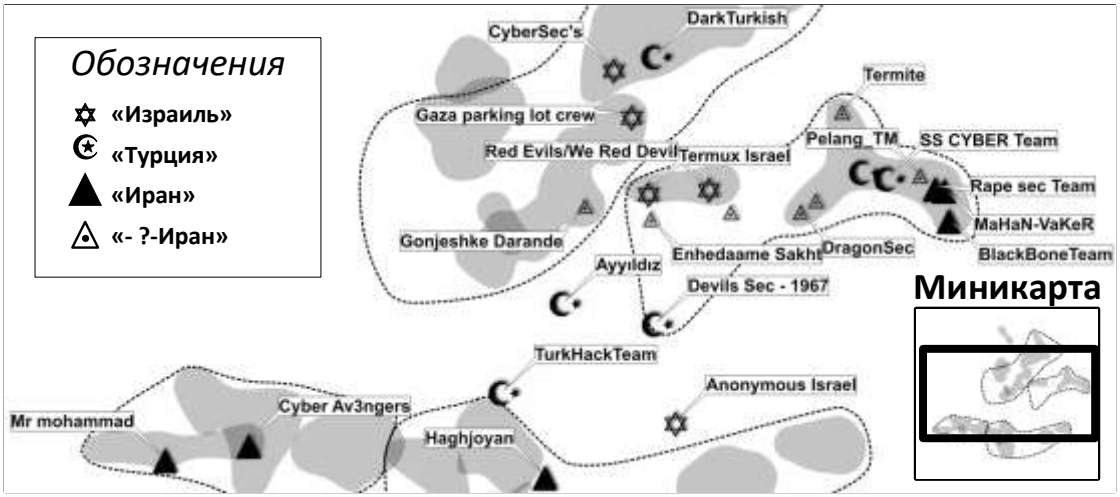

Рис.9. Хактивисты, связанные с Израилем, Турцией и Ираном

Данные группировки не образуют плотных кластеров, а рассредоточены по всей карте. Это обусловлено отсутствием альянсов из более мелких группировок. Также в центральную область карты попадают протурецкие хакерские группы, которые также не имеют сильно связанного сообщества из Telegram-каналов. Протурецкие хактивисты заняли активную позицию поддержки Палестины, однако сообщений о значимых взломах или распределённых атак от них зафиксировано не было.

Особое место занимают группировки, обозначенные на рис. 9 в виде пирамиды с точкой (такие группы, как Gonjeshke Darande, Tapandegan, DragonSec, Enhedaame Sakht/ Prana Network, Anonymous OpIran). Свои сообщения они публикуют на персидском и английском языках, а их действия направлены против действующей власти. Группы выражают интересы США и Израиля. Некоторые в прошлом отметились яркими атаками (например, в 2022 году Gonjeshke Darande нанесла ущерб компаниям сталелитейной промышленности Ирана, опубликовав в качестве подтверждения фотографии с видеокамер, на которых изображается нарушение техпроцесса, также были выложены конфиденциальные документы взломанных компаний). За рассматриваемый период некоторые группировки отметились в атаках на сайты государственных информационных систем Сирии и Ирана. Сообщения в поддержке Палестины или Израиля от данных групп зафиксированы не были.

От хактивистов, связанных с Ираном и Израилем поступали достаточно серьёзные сообщения об успешных атаках на критические объекты энергетической инфраструктуры. Например, проиранская группировка Cyber Av3ngers сообщала о взломе израильской частной электростанции Dorad, национальной водной компании Mekorot, а также городских очистных сооружений. Произраильская группа Red Devil информировала о выведении из строя большей части энергосистемы Ирана. Данные сообщения нуждаются в подтверждении. Также необходимо отметить, что некоторые сообщения о крупных утечках или взломах являются дезинформаций (например, архив с 37 Гб данных, выдаваемый проиранскими хактивистами Haghjoyan за результат взлома информационного ресурса спецслужбы Израиля Моссад оказался старой утечкой документов производителя аккумуляторов для военной техники Epsilor).

Заметной силой, участвующей во всех киберконфликтах, являются глобальные группировки хактивистов, которые объединяются на основании общих целей, а не государственной принадлежности, включают в свой состав участников из разных стран, используют в своих информационных сообщениях несколько языков, а объекты атаки относятся к различным регионам и отраслям (рис. 10). Их деятельность сложно отделить от деятельности киберпреступников, так как глобальные сетевые хактивисты имеют тесные связи в теневом сегменте Интернета, пользуются услугами и инфраструктурой финансово-мотивированных группировок (а иногда и формируют такую инфраструктуру).

Рассматриваемые субъекты распределены по всей карте. Некоторые из них выступают отдельными независимыми группировками (например, Moses Staff), но большинство объединены в сообщества (альянсы). Из наиболее активных альянсов можно выделить Anonymous, The Five Families, GhostClan, Killnet. Альянсы, как правило, на карте образуют собственный кластер. Исключение составляет одна из старейших групп – Anonymous. Она действует с 2003 года. Из-за своего медийного влияния превратилась в бренд, которые стараются использовать различные группировки. Децентрализованный и анонимный характер приводит к тому, что подобным группам очень сложно поддерживать общее ядро и представлять единую сторону в киберконфликтах. Группировки, использующие в своём названии слово «Anonymous», представлены во всех областях карты. Имеются группы, которые поддерживают как Палестину (например, Anonymous Sudan, Anonymous BD), так и Израиль (Anonymous India).

Данные группы отметились организацией DDoS-атак на критические объекты, например, координацией атаки на

систему противоракетной защиты «Железный купол».

Сообщения об атаке на данную систему начали поступали ещё весной 2023 года. VulzSec в своём Telegram-канале заявили о перехвате системы мониторинга «Железный купол» и получении доступа к данные их службы безопасности. 21 августа AnonGhost раскрыли IP-адреса системы. В дальнейшем данный перечень достаточно часто будет использоваться хакерскими группировками для проведения распределённых атак типа «отказ в обслуживании».

7 октября AnonymousSudan заявляет о начале атаки на критические точки в системе оповещения о ракетном нападении на Израиль, которые могут повлиять на систему «Железный купол», AnonGhost присоединился к атаке.

14 октября на форуме обсуждения утечек размещена информация о взломе израильской компании Mprest, занимающейся разработкой программного обеспечения для мониторинга, контроля и анализа в том числе для оборонного сектора.

15 октября ASKAR DDOS объявляет о планах атаковать систему. В этот же день от Brigade Syuhada Al-Aqsa поступает сообщение о том что военное подразделение Unit Militer 65, занимающееся кибер-операциями, в результате кибератак нарушили работоспособность некоторых информационных ресурсов раннего предупреждения, связанные с системой «Железный купол». Кроме того, утверждается, что были выведены из строя устройства управления в армейских объектах вдоль разделительной линии, а также взломаны камеры видеонаблюдения в поселениях вокруг сектора Газа. Сообщение распространилось по некоторым индонезийским хактивистким сообществам (в том числе AnonGhost Indonesian, GARNESIA).

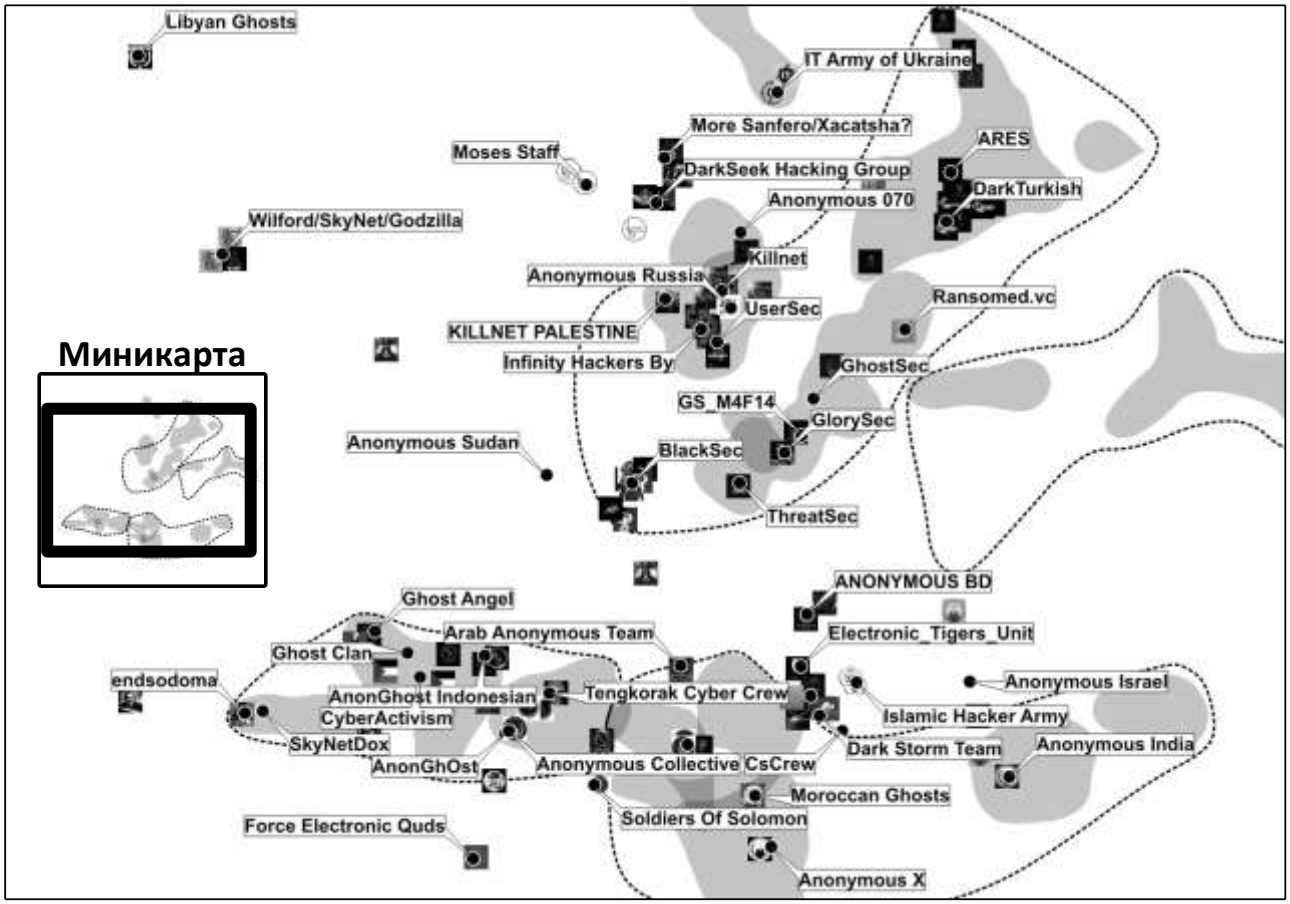

Рис. 10. Глобальные сообщества хактивистов и киберпреступников (Anonymous, GhostSec, GhostClan, Killnet, ARES и др.)

16 октября TEAM: ONE PIECE заявляет о взломе компании IBM ISAEL, в результате которого была получена конфиденциальная информация, в том числе более 5000 тысяч шифров для системы «Железный купол». Компания IBM ISAEL информацию о взломе опровергла. Также 16 октября поступают сообщение о планируемых атаках от хактивистов Islamic Hacker Army, AnonGhOst, Electronic_Tigers_Unit, Team R70. 18 октября в Telegram-канале турецких хакеров DarkTurkishTeam опубликованы фотографии и персональные данные 33 сотрудников Mprest. 22 октября GB ANON 17 разместил 225 документов, связанных с закупкой компонентов для системы «Железный купол».

Пример протяжённой, распределённой и неконденсируемой атаки на систему «Железный купол» наглядно показывает, как деятельность хактивистов из различных группировок, кластеров и альянсов может создавать реальную угрозу критически важным объектам в долгосрочной перспективе.

Заключение

Построенная в ходе исследования информационная карта киберконфликта «Палестина-Израиль» позволила наглядно представить противостояние в информационном пространстве различных сил, к которым относятся политически мотивированные группировки (хативисты). Основной площадкой для их информационной деятельности является социальная платформа Telegram. Благодаря информационной карте проведён анализ скрытых взаимосвязей между хактивистами (проявленных через объекты атак, цитирование сообщений и лингвистические особенности их содержимого). В ходе анализа было установлено, что киберконфликт «Палестина-Израиль» гораздо шире, чем противоборство двух сил (Израиля и Палестины). Он охватывает несколько стран из различных географических регионов и глобальные сетевые сообщества.

К сторонам киберконфликта можно отнести хактивистов, связанных с Израилем и Ираном, хактивистов стран Арабского и Индо-Тихоокеанского региона, а также глобальные сетевые группировки, связанные с киберпреступностью. Их взаимные противоречия (в том числе противоречия между мусульманскими странами и Израилем, между странами запада, Китая и Ирана, между Индией и граничащими с ней странами, а также между анонимными группировками хактивистов внутри хакерского сообщества) приводят к появлению множественных союзов, что повышает сложность анализа обстановки.

Наиболее яркими событиями в информационном пространстве, связанном с киберконфликтом «Палестина-Израиль», являются атаки на государственные объекты, имеющие как медийное, так и функциональное значение в военной, экономической и политической сферах. К таким событиям относятся сообщения об атаках на систему «Железный купол» Израиля и его энергетическую систему, а также сообщения об атаках на критические информационные объекты Ирана. При этом основной фон составляют сообщения о проведении распределённых атак типа «отказ в обслуживании» на многочисленные частные и государственные объекты, а также сведения об утечках персональных данных граждан и конфиденциальных документов коммерческих компаний сторон конфликта.

Применение метода информационного картографирования позволяет более эффективно решать задачи анализа оперативной обстановки за счёт систематизации и наглядного представления многочисленных сообщений о деятельности более 150 хактивистких группировок. Информационная карта обеспечивает возможность работы с данными в едином рабочем пространстве, что позволяет объединять усилия нескольких экспертов. Благодаря генерализации данных, масштабированию и возможности интерактивного анализа обеспечивается быстрое переключение внимания, что повышает концентрацию аналитика, снижает его когнитивную нагрузку и повышает скорость работы с данными.

В результате исследования сформирован набор данных о деятельности хактивистких группировок Арабского и Индо-

Тихоокеанского регионов за период с 6 октября по 11 ноября 2023 года, публиковавших сообщения в социальной платформе Telegram. Набор данных размечен в соответствии с результатами информационно-картографического анализа и может быть использован для решения задач в области искусственного интеллекта (например, для решения задачи классификации текстовых сообщений). Так как набор данных включает более 200 тыс. сообщений на различных иностранных языках и может содержать деструктивный контент (например, экстремистские высказывания хактивистов), доступ к нему ограничен. Для исследовательских целей набор данных можно запросить в редакцию журнала «Информация и безопасность».

В дальнейшем планируется продолжить информационно-картографическое исследование сил, действующих в рассмотренных регионах, ввиду важности соответствующих процессов для защищаемого информационного пространства Российской Федерации. Перспективными направлениями исследований являются:

- количественная оценка рисков реализации угроз, связанных с действиями хактивистов, на основе анализа статистики об инцидентах, зафиксированных в ходе информационно-картографического анализа;
- обоснование архитектуры и характеристик информационно-картографической системы мониторинга рисков киберугроз для защищаемого информационного пространства Российской Федерации;
- формирование наборов данных для задач автоматической выработки мер защиты от киберугроз с использованием технологий искусственного интеллекта.

Список литературы

1. Brangetto P., Veenendaal M. A. Influence cyber operations: The use of cyberattacks in support of influence operations // 2016 8th International Conference on Cyber Conflict (CyCon). – IEEE, 2016. – С. 113-126.

2. Cordey S. Cyber influence operations: An overview and comparative analysis // CSS Cyberdefense Reports. – 2019.

3. Сердечный А.Л. Киберпространство как объект исследования и защиты. часть 1 // Информация и безопасность. 2021. Т. 24. Вып. 3. С. 309-326.

4. Сердечный А.Л. Киберпространство как объект исследования и защиты. часть 2 // Информация и безопасность. 2021. Т. 24. Вып. 3. С. 327-348.

5. Сердечный А.Л. Информационная картография динамики тематической кластеризации каналов социальной сети Telegram в период проведения специальной военной операции вооруженных сил РФ на Украине // Информационный ресурс «Безопасный Интернет». URL: https://безопасный-интернет.рф/информационная-картография (дата обращения: 12.11.2023).

6. Остапенко А.Г. Картография защищаемого киберпространства / А.Г. Остапенко, А.Л. Сердечный, А.О. Калашников; Серия Теория сетевых войн; Вып. 7. [Под ред. чл.-корр. РАН Д.А. Новикова.

7. Israel-Palestine CyberTracker - 2NOV 2023 // Блог исследователя Cyberknow. URL: https://cyberknow.substack.com/p/israel-palestine-cybertracker-2nov (дата обращения: 12.11.2023).

8. Mayank S. The Evolving Landscape of Cyber Warfare in the Israel-Palestine Conflict: A Comprehensive Analysis // Блог компании Tsanct Technologies Pvt Ltd. URL: http://falconfeeds.io/blog/post/the-evolving-landscape-of-cyber-warfare-in-the-israelpalestine-conflict-a-comprehensive-analysis--356011 (дата обращения: 12.11.2023).

9. Репозиторий IsraelPalestineConflict // GitHub-репозиторий Giaimo Massimo. URL: https://github.com/fastfire/IsraelPalestineConflict (дата обращения: 12.11.2023).

10. Блог компании CYFIRMA URL: Israel Gaza Conflict: The Cyber Perspective URL: https://www.cyfirma.com/outofband/israel-gaza-conflict-the-cyber-perspective/ (дата обращения: 12.11.2023).

11. Boldi E. La geopolitica della cyberwarfare: i gruppi pro-Israele e quelli pro-Palestina // Giornalettismo URL: https://www.giornalettismo.com/la-geopolitica-

della-cyberwar-israele-hamas/ (дата обращения: 12.11.2023).

12. Битва хакеров в киберпространстве // URL: Платформа Telegraph (автор: НеКасперский) https://telegra.ph/Bitva-hakerov-v-kiberprostranstve-10-27 (дата обращения: 12.11.2023).

13. Israel-Cyber-Warfare-Threat-Actors // GitHub-репозиторий исследователей Deep Instinct URL: https://github.com/deepinstinct/Israel-Cyber-Warfare-Threat-Actors/tree/main (дата обращения: 12.11.2023).

Государственный научно-исследовательский испытательный институт
проблем технической защиты информации ФСТЭК России
State science research experimental institute of technical information protection
problem of Federal service of technical an export control

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 16.11.2023

Информация об авторах

Сердечный Алексей Леонидович – канд. техн. наук, начальник лаборатории, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России, e-mail: alex-voronezh@mail.ru

Остапенко Александр Григорьевич– д-р техн. наук, заведующий кафедрой, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

INFORMATION MAP OF THE CYBER CONFLICT “PALESTINE-ISRAEL”

A.L. Serdechnyi, A.G. Ostapenko

The processes of information warfare in cyberspace are closely related to the global political situation. The risks of computer attacks on government, industrial, financial and private information systems are increasing with the escalation of conflicts between states, including as a result of the intensification of politically motivated hackers (hacktivists). In recent years, this threat source has become a well-organized force capable of conducting complex and long-term operations, working in conjunction with cybercriminals and APT groups. This article presents the results of a study of the Palestine-Israel cyber conflict, which is aimed at identifying hidden connections between the subjects of the conflict under consideration. The study was conducted using the information mapping method, which made it possible to structure information from more than 150 hacktivist groups from the countries of the Arab and Indo-Pacific regions. As a result of the information and cartographic analysis, assessments of the situation in cyberspace in the regions under consideration were obtained, and a set of data on the activities of the corresponding hacktivist groups for the period from October 6 to November 11, 2023 was generated.

Keywords: hacktivists, information map, cyberwar, Palestine-Israel.

Submitted 16.11.2023

Information about authors

Alexey L. Serdechnyy – Cand. Sc. (Technical), Chief of Laboratory, State science research experimental institute of technical information protection problem of Federal service of technical an export control, e-mail: alex-voronezh@mail.ru

Alexander G. Ostapenko– Dr. Sc. (Technical), Head of the Department, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com