DOI 10.36622/VSTU.2023.4.26.011
УДК 004.056.47

МЕТОД ИНФОРМАЦИОННО-КАРТОГРАФИЧЕСКОГО АНАЛИЗА АКТИВНОСТИ ГРУППИРОВОК ХАКТИВИСТОВ

А.Л. Сердечный, А.Г. Остапенко

Объективное понимание ландшафта угроз является необходимым условием для выработки эффективных мер предотвращения компьютерных инцидентов или снижения негативных последствий в случае их наступления. В статье предлагается метод, который обеспечивает такое понимание для угроз, связанных с действиями политически мотивированных группировок (хактивистов). Метод основан на использовании информационных карт для визуализации сложных взаимосвязей между такими группами. В рамках описания метода определён процесс построения и анализа информационных карт, включающий сбор сведений о действиях хактивистов в публичном пространстве, формирование графа связей и размеченного ландшафта информационной карты, с помощью которых проводится анализ явных и скрытых зависимостей между группировками, их сообществами, а также атакуемыми объектами. С помощью информационных карт удобно осуществлять мониторинг за большим количеством источников и событий в рамках глобальных киберконфликтов, затрагивающих несколько сотен групп из различных стран и регионов. В результате информационно-картографического анализа активности группировок хактивистов могут быть заранее определены направления их атак, что позволяет своевременно повысить бдительность групп реагирования на инциденты и обеспечить координированное взаимодействие в информационном пространстве.

Ключевые слова: информационно-картографический анализ, хактивисты, информационная карта.

Введение

Одним из первых этапов оценки рисков реализации угроз безопасности информации является сбор полных и достоверных данных об источниках угроз, что невозможно без объективного понимания обстановки для зоны киберпространства, в которой находится объект защиты [1]. В киберпространстве оценка обстановки осложняется повышенной динамичностью данной среды и отсутствием чёткого определения территорий и границ действия различных субъектов [2, 3]. Изменение обстановки определяется множеством условий и факторов, сказывающихся на ландшафте угроз. Если в одних условиях объект защиты не представляет интереса для злоумышленников, то в случае их изменения он может стать одной из актуальных целей, что оказывает существенное влияние на вероятность реализации угрозы.

Так, например, в обычное время объекты мелкого и среднего бизнеса или региональные некоммерческие организации, средства массовой информации и информационные ресурсы органов власти могут не представлять интереса для финансово мотивированных киберпреступников, приносящих наибольший ущерб.

Во время обострения киберконфликтов возрастает доля атак со стороны хактивистов, для которые такие объекты служат достаточно лёгкими целями [4-6]. Периодические атаки на такие объекты создают эффект постоянного присутствия в информационном пространстве. Взлом слабо защищённых целей также способствует формированию сообщества последователей из группировок с низкими возможностями, для которых такие объекты являются единственной возможностью отметиться в качестве активной силы киберконфликта.

Для атакуемых организаций ущерб от такой деятельности может быть достаточно ощутимым, так как в результате успешных атак возможно попадание в открытый доступ защищаемой информации. Также возможна

потеря клиентов из-за репутационных издержек, вызываемых публикациями журналистов или снижением качества предоставляемых услуг по причине продолжительных DDoS-атак.

Кроме того, для крупных организаций, привыкшим к атакам со стороны APT-группировок и киберпреступников, может оказаться неожиданным массовое скоординированное нападение большого числа политически-мотивированных групп, которые одновременно и сразу по нескольким направлением оказывают давление на службу безопасности. В результате отвлечения ресурсов на многочисленные действия хактивистов может произойти перегрузка системы защиты (например, отказ какого-либо из её компонентов или заполнение журнала безопасности избыточным количеством сообщений об инцидентах) может способствовать проникновению других видов злоумышленников, которые используют деятельность хактивистов как операцию прикрытия.

В связи с этим исследование деятельности политически мотивированных группировок в рамках оценки рисков реализации угроз безопасности информации является актуальной задачей, однако для её решения необходимо фиксировать и сопоставлять множество фактов о составе, структуре и функциональных возможностях хактивистов и их альянсов (объединений), что наиболее сложно сделать в условиях крупномасштабных киберконфликтов (примерами которых являются киберконфликты «Россия-Украина», «Палестина-Израиль»), в которых задействованы сотни групп из различных стран и регионов.

Использование технологий искусственного интеллекта для облегчения решения этой задачи за счёт автоматического анализа потока сообщений об активности хактивистов в настоящее время не представляется возможным ввиду отсутствия в открытом доступе качественных наборов данных и моделей машинного обучения для классификации таких сообщений по виду хактивистской деятельности, а также соотнесение их с названиями хактивистких групп, атакуемых объектов, способов реализации компьютерных атак и других характеристик событий.

Для преодоления данного противоречия был разработан метод информационно-картографического анализа, описание которого представлено в настоящей статье.

Хактивисты как объект информационно-картографического анализа

Явление «хактевизм» было описано в конце XX-го века [7], еще до того, как развитие Интернета стало настолько масштабным, что охватило практически все сферы жизни человека. Данный термин обозначает деятельность субъектов в киберпространстве, мотивом которой является достижение политических целей в рамках реализации какой-либо идеи.

Данный мотив определяет различные стратегии поведения хактивистов, отличающиеся от стратегий остальных субъектов (киберпреступников, APT-группировк, кибервойск) обязательным наличием информационных площадок, через которые они пропагандируют свои идеи и отчитываются о результатах проделанной работы [4-8].

Хактивизм может принимать различные формы, которые в некоторых случаях сложно отличить от киберпреступлений [9] или кбиертерроризма (впервые термин использован в середине 1980-х годов для обозначения возможных террористических действий в виртуальном пространстве) [7, 10].

Во многих работах (например, [11,12]), группировки хактивистов рассматриваются как инструмент «мягкой силы», который помогает государствам через информационное пространство оказывать влияние на политические процессы своих противников. Однако, как можно видеть на практике, в случае возникновения военных конфликтов группы хактивистов помимо оказания информационно-психологических воздействий, выступают активной силой в проведении разведывательных и диверсионных операций на военную и критически важную информационную инфраструктуру противника [5, 6], что

нехарактерно для инструмента «мягкой силы», а больше свойственно кибервойскам.

В работе [3] автор ставит под сомнение само понятие «Кибервойна», а явление хактивизма рассматривается как объединение на новой технологической основе трёх традиционных видов деятельности: саботажа, шпионажа и подрывной деятельности.

Можно выделить следующие виды хактивисткой деятельности:

а) целевые:

- получение несанкционированного доступа к информационным системам;
- проведение атак типа «отказ в обслуживании»;
- оказание информационно-психологического воздействия;
- расследование утечек и публикация информации ограниченного доступа;

б) обеспечивающие:

- обеспечение инфраструктуры для распространения информации и анонимного взаимодействия участников хактивисткого движения;
- разведка по открытым источникам и анализ утечек;
- разработка инструментальных средств для проведения кибероперациий;
- привлечение в свои ряды и обучение новых членов;
- подготовка мультимедийных материалов.

Целевые виды деятельности напрямую связаны с выражением идеи, которую преследует группа хактивистов.

Хактивисты, выступающие за свободу слова, в большей степени склонны публиковать информацию, полученную в результате несанкционированного доступа. В сотрудничестве с ними действуют журналисты-расследователи, которые опираются на информацию, полученную незаконным способов и предоставленную им для анализа. Частота публикаций сообщений такими группами достаточно низкая, однако качество проделываемой работы и уровень возможностей хактивистов чрезвычайно высоки.

Хактивисты, целью которых является противодействие какому-либо негативному явлению, сконцентрированы на проведении атак типа «отказ в обслуживании». Данную деятельность можно разделить на два типа:

- взлом и нарушение работы хорошо защищённых объектов;
- проведение DDoS-атак на информационные ресурсы небольших организаций.

Взлом и выведение из строя хорошо защищённых объектов также требует от хактивистов высокого уровня профессионализма. Проведение распределённых атак типа «отказ в обслуживании» обычно не требует мастерства участников, а выражается лишь в использовании их вычислительных ресурсов и особого положения (наличие доступа во внутренние сегменты, где располагаются атакуемые объекты). Эффект достигается за счёт массовости обращений от разнородных субъектов, напоминающих легитимных пользователей. Для них трудно определить демаскирующие признаки, соответственно, сложно заблокировать, не нарушив штатную работу своей системы. При этом необходимо отметить, что для успешного проведения DDoS-атак на веб-сайты, находящиеся под защитой крупных CDN-сетей, требуется привлечение очень мощных ресурсов, что требует от хактивистов наличие множества ботнетов (сетей устройств, захваченных и контролируемых злоумышленниками).

Публикация результатов журналистких расследований и сообщений об успешных деструктивных атаках являются информационно-психологическим воздействием, однако со стороны хактивистов могут предприниматься и другие воздействия, к которым относятся:

- публикация персональных данных граждан;
- деанонимизация оппонентов («доксинг» от англ. doxing);
- «дефейс» (изменение) заглавной страницы сайта или размещение на нём компрометирующей информации.

Для реализации указанных воздействий группировки хактивистов должны заниматься *обеспечивающими видами* деятельности.

Обеспечение инфраструктуры для распространения информации и анонимного взаимодействия участников хактивисткого

движения предполагает создание и ведение собственных сайтов или каналов в социальных платформах. Такие ресурсы должны быть хорошо защищены, так как в случае успешности хактивистов они являются уязвимым местом. Их взлом может привести к разоблачению хактивистов или блокированию информационной деятельности.

Важным видов деятельности является разведка по открытым источникам и анализ утечек, которая проводится хактивистами для выбора объекта атаки и получения о нём предварительной информации.

Разработка инструментальных средств для проведения кибероперациий связана с выявлением уязвимостей «нулевого дня» (уязвимостей программного обеспечения, для которых разработчик не выпустил обновления, которое должно их устранить), созданием модулей взаимодействия с командными северами, подготовкой вредоносного программного обеспечения, способного преодолевать механизмы защиты, созданием и развёртыванием фишинговых сайтов и др.

Привлечение в свои ряды новых членов и их обучение, а также подготовка качественных мультимедийных материалов требуется хактивистам, которые стремятся расширить своё влияние и образовать альянсы со сложной структурой. Эта деятельность направлена на расширение аудитории для более эффективного распространения своих идей, а также на получение дополнительных ресурсов, позволяющих проводить более сложные операции.

Отдельно стоит отметить важность выбора символики группы. Благодаря логотипам, названию, образу и стилю хактивистов осуществляется их различие. Это приводит к тому, что члены группировок могут быть деанонимизированы на основании особого почерка, проявляемого в используемых символах. С другой стороны, в условиях анонимности, оппоненты группировок могут успешно подделать стиль, название и логотип группы для последующей компрометации хактивистов.

На основании представленного описания можно утверждать, что «хактивизм» является достаточно сложным явлением, оказывающим существенное воздействие на ландшафт угроз. В момент международной нестабильности, но до начала полномасштабной кибервойны, хактивисты являются наиболее активной силой, которую следует исследовать и учитывать при моделировании угроз и расчёте рисков. Существующие примеры киберконфликтов «Россия-Украина» и «Палестина-Израиль» [5, 6] показывают, что в них могут принимать участия сотни различных группировок со своими идеями и целями.

Для понимания соответствующих процессов требуются особые теоретические и инструментальные средства, с помощью которых может быть обеспечен анализ и понимание больших объёмы информации. В рамках настоящего исследования основой таких средств выступает методология информационного картографирования [2]. Её применение к процессу исследования деятельности хактивистов позволило разработать метод построения и анализа системы информационных карт, с помощью которых такая деятельность представляется в наглядной и интерпретируемой для человека форме. Метод может быть реализован с помощью информационно-картографической системы [13].

Практическая апробация метода проводилась для группировок хактивистов из стран Арабского и Индо-Тихоокеанского регионов. Для этого с помощью системы картографирования рисков [14] была построена информационная карта киберконфликта «Палестина-Израиль», с помощью которой были получены оценки обстановки, сложившейся в киберпространстве рассматриваемых регионов в период с 6 октября по 11 ноября 2023 года.

Сущность метода информационно-картографического анализа активности группировок хактивистов

Разработанный метод схематично можно представить в виде циклического выполнения трёх видов работ (рис. 1):

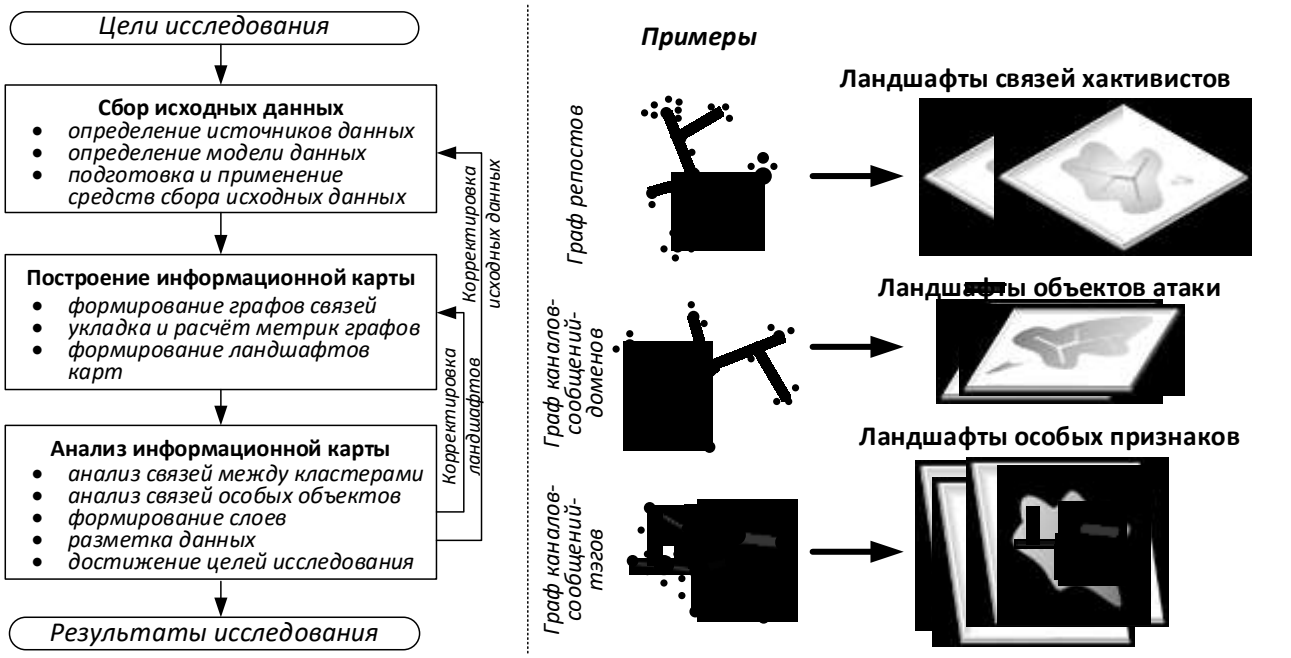

Рис.1. Схема проведения информационно-картографического анализа

- сбора исходных данных;
- построения информационной карты;
- анализ информационной карты.

Работы выполняются для системы информационных карт с различными слоями и ландшафтами, которые удобно использовать для достижения той или иной цели исследования.

Цели исследования, которые можно достичь с помощью разработанного метода, напрямую связаны с задачами информационного-картографирования, изложенными в [2]. К ним относятся:

- мониторинг деятельности хактивистов с помощью информационных карт (задача «Мониторинг обстановки»);
- систематизация событий, связанных с действиями хактивистов (задача «Представление знаний»);
- определение состава, структуры и взаимоотношений между группировками хактивистов (задача «Картографическая разведка»);
- планирование мероприятий в отношении снижения риска реализации угроз со стороны хактивистов с помощью информационных карт (задача «Планирование операций»).

Для их достижения может потребоваться несколько информационных карт. Уникальность информационной карты определяется её ландшафтом, который строится на основании графа связей между объектами, с помощью которых выражаются определённые аспекты деятельности хактивистов.

На первом шаге реализации метода выполняется сбор исходных данных. Для этого определяются возможные источники, формируется единая модель данных, для сведений из различных источников, подготавливаются инструментальные средства.

Источниками исходных данных в первую очередь являются информационные ресурсы хактивистов. На сегодняшний день большинство хактивистов пользуются услугами социальных платформ Telegram и X/Twitter (последней в меньшей степени из-за политики цензуры владельцев Twitter). Некоторые хактивисты доверяют только собственному сайту, который может быть расположен в пространстве анонимных децентрализованных сетей типа Tor или I2P.

В качестве дополнительных источников рассматриваются научные публикации и отчёты экспертов, в которых представлены результаты исследования деятельности хактивистов. Такие источники могут рассказать о деятельности группировок, которая не афишируется на их официальных ресурсах.

Модель данных должна обеспечивать единую форму представления сведений из

различных источников. Она может быть выражена как в виде таблиц в терминах реляционной модели баз данных, так и с помощью графов свойств, используемых в графовых базах данных.

Сбор данных может проводиться как в автоматическом, так и в ручном режимах. Большинство данных собирается с помощью специально разработанных модулей (парсеров), загружающих и преобразующих данные из формата источника в формат, определяемый моделью данных. Часть данных (например, информация об отношениях между группами хактивистов) из неструктурированных источников, может быть собрана вручную.

После сбора данных выполняется второй шаг – формирование ландшафта информационной карты. Для различных целей исследования могут использоваться различные ландшафты. Ландшафтом карты представляет собой граф, уложенный в двухмерном или трёхмерном пространстве с помощью силовых методов (например, с помощью алгоритма ForceAtlas2), с размеченными зонами, в которые попадают узлы или их скопления, обладающие схожими свойствами. Автоматизация разметки карты может быть осуществлена с помощью алгоритмов кластеризации графа, интерполяции для построения тепловой карты. Для автоматического определения меток кластеров могут использоваться методы машинного обучения, с помощью которых выявляются общие свойства узлов, попавших в один кластер.

На третьем шаге проводится анализ информационной карты, включающий:

- выявление структурных особенностей графа, лежащего в основе ландшафта (связи и расположения кластеров);
- изучение отдельных узлов, для которых были рассчитаны и визуально представлены значения метрик и свойств (например, через значение метрики центральности узла PageRank, выраженное в его размере, могут быть обнаружены наиболее влиятельные группировки в рамках определённой области ландшафта карты);
- формирование слоёв, с помощью которых визуализируется дополнительная информация (потребность в слоях возникает из-за необходимости скрыть лишние детали, избыточные для текущей задачи анализа).

В ходе анализа может быть установлено, что текущий ландшафт и исходные данные недостаточно полно и точно отражают сложившуюся обстановку. Например, в процессе изучения структурных особенностей графа определено, что перечень рассмотренных группировок не полон, так как существуют косвенные признаки наличия в определённой области карты дополнительного субъекта. В этом случае такой субъект должен быть выявлен, исходные данные о его связях дополнены, а ландшафт при необходимости скорректирован (если появление новой информации существенно не влияет на структуру кластеров, то такие данные можно поместить на текущий ландшафт без необходимости его полной перестройки).

Шаги выполняются для каждого ландшафта. Совокупность ландшафтов вместе образуют систему карт (атлас) по теме исследования. Каждый из ландшафтов строится под конкретную задачу исследования. Так, например, для определения состава, структуры и взаимоотношений между группировками хактивистов удобнее всего использовать ландшафт связей хактивистов, проявляемых во взаимном цитировании сообщений между дружественными группировками. Такие связи могут быть представлены графом репостов сообщений из Telegram-каналов хактивистов (рис. 2).

Ландшафт объекта атаки позволяет систематизировать сведения об инцидентах с учётом типизации целей, которые выбирают хактивисты (рис. 3-А).

Названия операций хактивистов, обычно, указываются в виде хэштэга, прикреплённого к соответствующему информационному сообщению. Некоторые альянсы также с помощью хэштэгов перечисляют названия группировок, принимавших участие в операции (рис. 3-Б). Ландшафт хэштэгов показывает наиболее распространённые цели с учётом взаимоотношений между группировками.

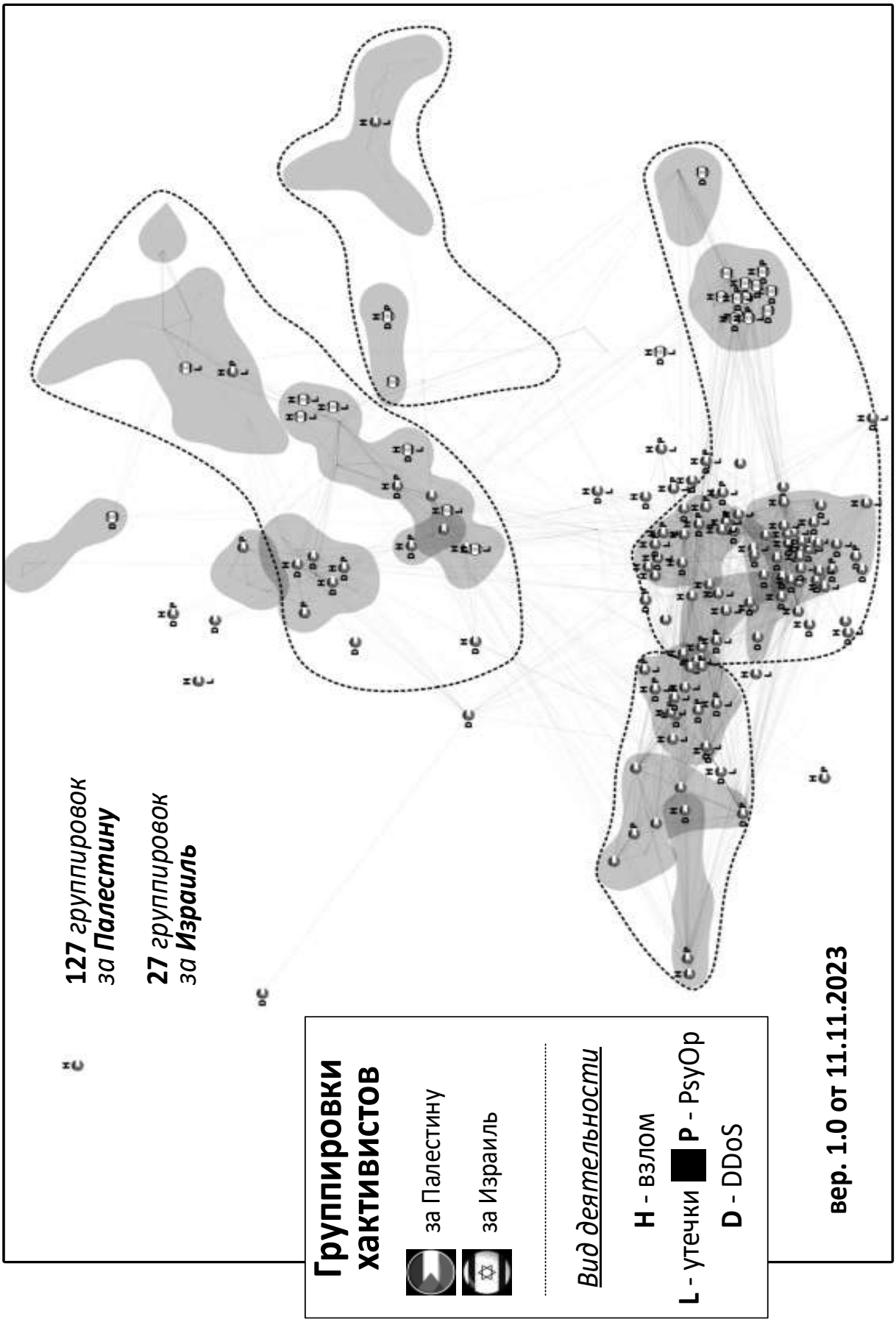

Рис. 2. Пример информационной карты с ландшафтом связей хактивистов (сторон киберконфликта «Палестина-Израиль») и отметками «Вид деятельности»

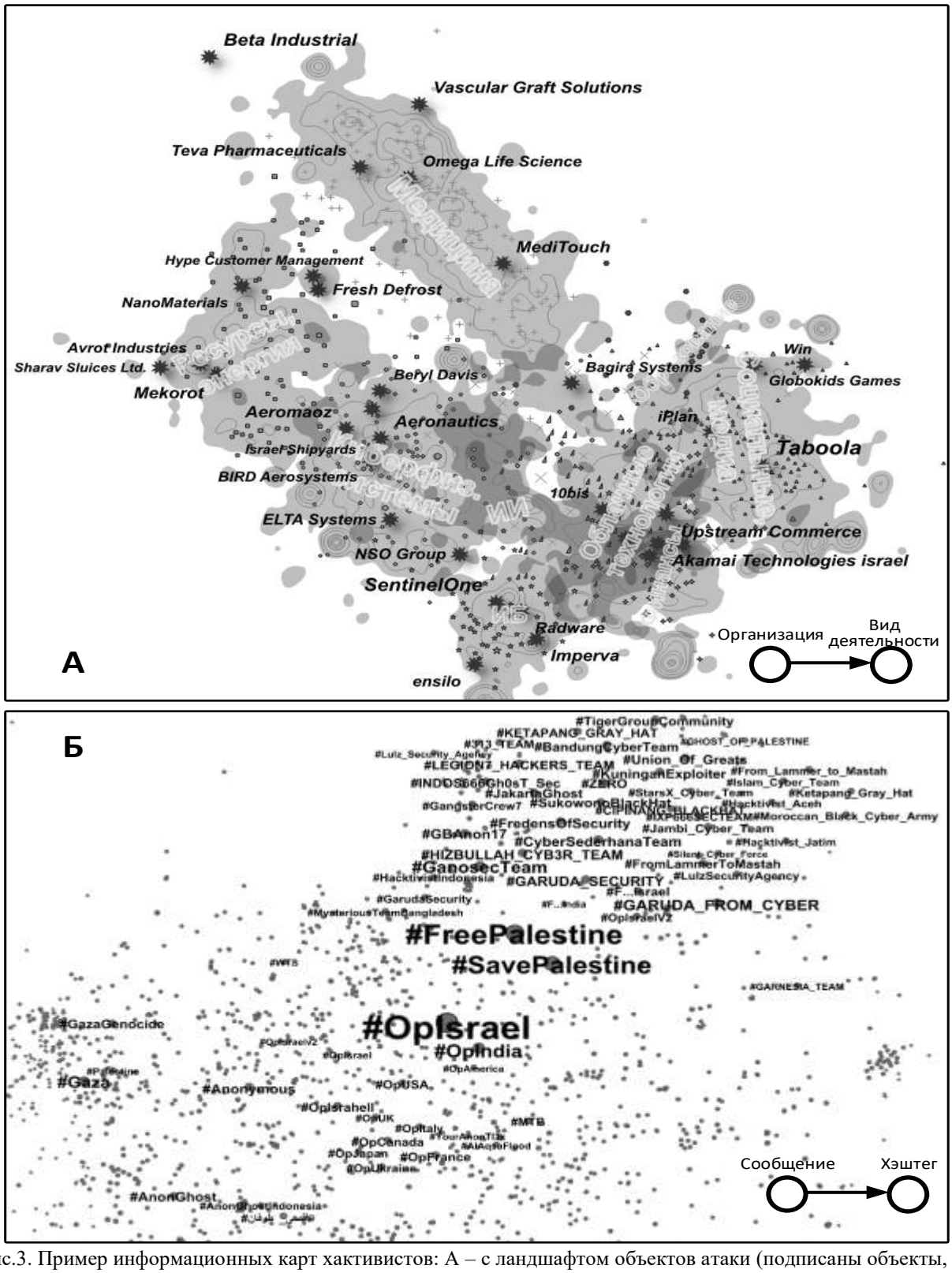

Рис.3. Пример информационных карт хактивистов: А – с ландшафтом объектов атаки (подписаны объекты, на которых проводились атаки); Б – с ландшафтом особых признаков (хэштегов)

Центральное место на карте (рис. 3-Б) занимаются хэштэги операций. В верхней правой части располагается большой кластер из названий хактивистов Арабского и Индо-Тихоокеанского регионов, которые хорошо взаимодействуют между собой, образуя альянс мусульманских хактивистов. Хэштэги произраильских группировок не представлены, так как соответствующие группировки их практически не используют.

Заключение

В настоящей работе предложен метод информационно-картографического анализа активности группировок хактивистов, заключающийся в построении и анализе системы информационных карт, с помощью которых фиксируются и наглядно представляются множество фактов о составе, структуре и функциональных возможностях хактивистов и их объединений.

Возможности метода обеспечивают решение следующих задач исследования активности хактивистов:

- мониторинг деятельности хактивистов с помощью информационных карт;
- систематизация событий, связанных с действиями хактивистов;
- определение состава, структуры и взаимоотношений между группировками хактивистов;
- планирование мероприятий в отношении снижения риска реализации угроз со стороны хактивистов с помощью информационных карт.

С помощью метода могут быть получены размеченные наборы данных для расчёта рисков реализации угроз безопасности информации, связанных с рассматриваемым типом субъектов, что было продемонстрировано на примере киберконфликта «Палестин-Израиль».

Дальнейшим развитием предлагаемого метода является совершенствование алгоритма расчёта и визуализации риска реализации угроз со стороны хактивистов с помощью информационных карт в реальном режиме времени.

Список литературы

1. Klipstein M. S., Naval Postgraduate School Monterey United States. Quantifying risk for decentralized offensive cyber operations: дис. – Ph. D. dissertation, Naval Postgraduate School, Monterey, CA, USA, 2017.

2. 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.

3. Rid T. Cyber war will not take place // Journal of strategic studies. – 2012. – Т. 35. – №. 1. – С. 5-32.

4. Naibo G. The reality of cyber warfare: The Ukraine-Russia conflict as a catalyst for new dynamics in cyberspace. – 2022.

5. Блог исследователя Cyberknow // Платформа Substack. URL: https://cyberknow.substack.com/ (дата обращения: 12.11.2023).

6. Блог компании Tsanct Technologies Pvt Ltd. // Информационный ресурс Falconfeedsio. URL: http://falconfeeds.io/blog/ (дата обращения: 12.11.2023).

7. Manion M., Goodrum A. Terrorism or civil disobedience: toward a hacktivist ethic //Acm Sigcas Computers and Society. – 2000. – Т. 30. – №. 2. – С. 14-19.

8. Romagna M. Hacktivism: Conceptualization, techniques, and historical view // The Palgrave handbook of international cybercrime and cyberdeviance. – 2020. – С. 743-769.

9. Farmer F. Cybercrime vs Hacktivism: Do we need a differentiated regulatory approach?. – University of Exeter (United Kingdom), 2022.

10. Капто А. С. Кибервойна: генезис и доктринальные очертания // Вестник Российской академии наук. – 2013. – Т. 83. – №. 7. – С. 616-616.

11. 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.

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

13. Сердечный А.Л. Информационно-картографические системы как инструментальная основа картографии защищаемого киберпространства // Системы управления и информационные технологии. 2021. № 4 (86). С. 41-46.

14. Сердечный А.Л. К вопросу о создании платформы картографирования рисков защищаемого киберпространства / А.Л. Сердечный, А.А. Гончаров, М.А.

Булычев и др. // Информация и безопасность.
2021. Т. 24. Вып. 4. С. 593-600.

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

THE INFOCARTOGRAPHIC ANALYSIS METHOD OF HACKTIVIST ACTION

A.L. Serdechnyi, A.G. Ostapenko

An objective understanding of the threat landscape is a prerequisite for developing effective measures to prevent computer incidents or reduce negative consequences in the event of their occurrence. The article proposes a method that provides such an understanding for threats related to the actions of politically motivated groups (hacktivists). The method is based on the use of information maps to visualize complex relationships between such groups. As part of the description of the method, the process of constructing and analyzing information maps is defined, including collecting information about the actions of hacktivists in public space, forming a graph of connections and a marked landscape of the information map, with the help of which the analysis of explicit and hidden dependencies between groups, their communities, as well as the attacked objects is carried out. With the help of information maps, it is convenient to monitor a large number of sources and events within the framework of global cyber conflicts affecting several hundred groups from different countries and regions. As a result of the infocartographic analysis of the activity of hacktivist groups, the directions of their attacks can be determined in advance, which makes it possible to increase the vigilance of incident response teams in a timely manner and ensure coordinated interaction in the information space.

Keywords: infocartographic analysis, hacktivists, information map.

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