DOI 10.36622/VSTU.2022.25.1.007
УДК 004.056.57

КАРТОГРАФИРОВАНИЕ КИБЕРПРОСТРАНСТВА И ЗАЩИТА ИНФОРМАЦИИ

А.Г. Остапенко, А.Л. Сердечный, С.Д. Трубицын, Д.А. Нархов, В.Ю. Остапенко

В статье рассматривается обеспечение ситуационной осведомленности об угрозах безопасности информации и компьютерных атаках с использованием центров реагирования на инциденты и информационных карт, включая ситуационные центры управления кибербезопасностью. Вышеуказанная осведомленность иллюстрируется информационными картами APT-группировок, отражающими состав жертв и заинтересованных в них атаке строк; артефакты в коде вредоносного программного обеспечения; атрибуцию группировки на основании авторского стиля написания программных средств реализации компьютерных атак. В этой связи представлены общие планы информационных карт для разнообразных APT-группировок. При этом обсуждается противодействие киберпреступности с использованием информационных карт. Обсуждается анализ финансовых операций злоумышленников в виртуальном пространстве за счет использования криптовалют. На примерах Blockchain и Bitcoin-транзакций рассматривается определение принадлежности криптокошельков. С помощью графа связей иллюстрируются вышеупомянутые транзакции. Предлагается также анализ вредоносного программного обеспечения как инструмента кибератак. В этой связи рассматривается информационная карта связей способов реализации компьютерных атак и объектов воздействия, построенная на основании онтологии.

Ключевые слова: ситуационная осведомленность, информационная карта, кибербезопасность, криптовалюта, транзакции.

Введение

Решение многих задач защиты информации связано с необходимостью анализа больших связанных данных. Так, например, в ходе расследования инцидентов, чтобы восстановить картину атаки требуется обнаружить и связать множество данных, полученных как от средств защиты информации, так и из дополнительных источников. Причём для их интерпретации требуется наличие соответствующих справочных баз, среди которых базы семейств вредоносного программного обеспечения, базы IP-адресов, базы bitcoin-кошельков и др.

На более низком (в плане детализации фактов) уровне, связанном с выявлением уязвимостей программного обеспечения, требуется проводить анализ графовых представлений программ, таких как абстрактные синтаксические деревья, графы вызовов функций, графы потока управления, графы зависимостей по данным.

Наличие соответствующих информационных карт не только позволяет систематизировать подобные связанные данные, но и использовать их совместно с другими исследователями.

Информационные карты могут повысить эффективность решение задач по следующим направлениям:

- ситуационная осведомлённость об угрозах безопасности информации и обнаружение компьютерных атак;
- противодействие компьютерной преступности;
- анализ вредоносного программного обеспечения;
- выявление уязвимостей программного обеспечения и программно-аппаратных средств.

Рассмотрим более подробно каждое направление.

Ситуационная осведомлённость об угрозах безопасности информации и обнаружение компьютерных атак

Современные угрозы безопасности информации достигли такого уровня развития, что для парирования требуется построение комплексной эшелонированной системы защиты. Подобные угрозы стали

актуальны не только для крупных организаций, но и для предприятий среднего масштаба. Эффективная защита от целенаправленных долговременных угроз (advanced persistent threat, далее – APT-угрозы) уже не может быть осуществлена только с использованием традиционных мер защиты, таких как межсетевые экраны и средства антивирусной защиты. Должны предприниматься активные действия при обнаружении первых признаков воздействия со стороны APT-группировок. Для этого требуется знание оперативной обстановки вокруг защищаемой информационной системы и непрерывный мониторинг как собственной инфраструктуры, так и общей активности со стороны злоумышленников, которые представляют реальную опасность для защищаемой системы.

Такая задача решается в рамках обеспечения ситуационной осведомлённости с использованием ситуационных центров и групп реагирования на инциденты. Практика построения современных ситуационных центров предполагает наличие мощной системы визуализации, с которой связаны аналитические системы организации. Ситуационные центры обрабатывают сигналы от различных типов средств защиты благодаря работе систем управление событиями информационной безопасности (SIEM-систем). В состав системы визуализации входит комплект интерактивных графических панелей, на которые выводятся таблицы, графики и географические карты с интегральными и частными показателями обстановки [1, 2, 3] (рис. 1).

Рис. 1. Ситуационный центр управления кибербезопасностью [3]

Информационные карты позволяют в более компактном виде передать наиболее полную информацию о представляющих интерес событиях безопасности. Однако для их эффективного применения требуется выбор походящих форм с учётом специфики решаемой задачи. Примеры задач в рамках обеспечения ситуационной осведомлённости об угрозах безопасности информации приведены в табл. 1.

Таблица 1

Примеры задач обеспечения ситуационной осведомлённости, решаемых с использованием информационных карт

Задача информационной картографии	Задача обеспечения ситуационной осведомлённости
Разведка	
Исследование неизведанных территорий	Выявление новых источников и новых классов компьютерных атак

Продолжение табл. 1

Задача информационной картографии	Задача обеспечения ситуационной осведомлённости
Выявление скрытых структур и элементов	Выявление связей между методами, способами и средствами APT-группировок, определение сценариев реализации компьютерных атак
Выявление противоборствующих сторон	Атрибуция APT-группировок
Планирование операций	
Анализ ресурсов противоборствующих сторон	Определение возможностей атакующих APT-группировок
Прокладка маршрута	Исследование способов компьютерных атак, оценка вероятностно-временных характеристик реализации компьютерных атак
Прогнозирование обстановки	Оценка рисков реализации угроз безопасности информации, определение наиболее вероятных объектов компьютерных атак, разработка мер защиты от угроз безопасности информации
Мониторинг обстановки	
Координация взаимодействия	Координация действий в рамках активного противодействия реализации угроз безопасности информации, проведение тестирования на проникновение
Задача информационной картографии	Задача обеспечения ситуационной осведомлённости
Выявление изменений обстановки	Обнаружение компьютерных атак, выявление уязвимостей информационных систем, оценка состояния защищённости в результате модернизации информационной системы
Выявление ошибок и дезинформации	Обнаружение противоречий между различными источниками сведений об APT-группировках, оценка эффективности ложных информационных систем
Представление знаний	
Обучение	Обучающие информационные карты по мерам защиты от компьютерных атак, визуализация киберучений и соревнований «Захват флага» (Capture the Flag)
Структурированное хранение знаний	Ведение баз APT-группировок и инцидентов информационной безопасности
Картографический поиск информации	Выявление новых источников сведений о методах, способах и средствах реализации компьютерных атак

Информационные карты APT-группировок

Ситуационная осведомлённость о глобальных угрозах безопасности информации заключается в отслеживании деятельности APT-группировок. Данный вид угроз представляет наибольшую опасность, так как реализуется нарушителями, обладающими высоким потенциалом. В качестве субъектов реализации целенаправленных долговременных угроз выступают спецслужбы передовых государств, а также представители транснациональных корпораций и, так называемые, «хактевисты» (анонимные киберпреступные группировки, преследующие политические цели).

Существуют следующие источники данных об APT-группировках:

- отчёты исследователей, в области защиты информации (в основном, разработчиков средств антивирусной защиты), в которых содержатся сведения о способах и средствах, используемых APT-группировками;
- отчёты об инцидентах безопасности информации;
- агрегированные данные, полученные на основе анализа открытых источников;
- платформы для обмена информацией об APT-группировках и вредоносном программном обеспечении.

В отчётах представлена подробная техническая информация и первичные исходные данные. Обычно такие сведения слабо формализованы и не имеют единых идентификаторов, позволяющих провести сопоставление данных между различными

источниками. Однако в последнее время получила развитие тенденция опубликования идентификаторов компрометации [4, 5, 6] вместе с отчётами. Это способствует формализации данных об APT-группировках.

Разнообразие подобных отчётов привело к появлению интеграторов, осуществляющих анализ и обобщение содержимого таких отчётов. Одним из крупных источников, агрегирующих сведений о методах, способах и средствах APT-группировок, является база знаний MITRE ATT&CK [7]. Также можно отметить базу знаний MISP [8] и проект APT Groups and Operations [9], в рамках которых проводится экспертная обработка отчётов с первичными данными о постоянных целенаправленных угрозах.

В рамках академических исследований разрабатываются средства автоматизированного анализа открытых источников на предмет поиска и извлечения информации о деятельности APT-группировок [10].

В настоящий момент известно более 1200 оригинальных исследований, содержащих результаты анализа методов, способов и средств реализации APT-угроз [11]. Каждый из исследователей самостоятельно определяет имя APT-группировки на основании тех фактов, которые были выявлены в процессе исследования. Это могут быть особенные фрагменты строк, найденные в коде инструментальных средств (например, «Duqu»), которые были использованы для атаки, либо же уникальные идентификаторы в рамках внутренней системы хранения информации о целенаправленных атаках (например, APT3).

Ещё более сложной задачей в ходе исследования целенаправленных атак является установление принадлежности группировки к конкретной организации или стране. Основными способами решения этой задачи являются:

- анализ состава жертв с целью выявления заинтересованных сторон в их атаке;
- выявление артефактов в коде вредоносного программного обеспечения (текстовые строки и язык их написания, жаргонные слова, электронные адреса, доменные имена, идентификаторы bitcoin-кошельков и др.) [4, 5, 12];
- атрибуция APT-группировок на основании авторского стиля написания программных средств реализации компьютерных атак [5, 13, 14].

Для систематизации сведений об APT-группировках была разработана информационная карта, сведения о которой представлены в табл. 2.

Таблица 2

Сведения об информационной карте «APT-группировки»

Тип сведений	Характеристика информационной карты
Уровень	Уровень субъектов компьютерных атак, относящийся к социальному уровню киберпространства
Решаемые задачи	Выявление противоборствующих сторон, анализ ресурсов противоборствующих сторон, прокладка маршрута, прогнозирование обстановки, координация взаимодействия, выявление изменений обстановки, выявление ошибок и дезинформации, обучение, структурированное хранение знаний
Исходные данные	Объединение следующих наборов данных: - база знаний MITRE ATT&CK [7]; - наборы данных на основе стандарта MISP [8] (Threat Actor Map [15] и Malpedia [16]); - базы данных исследователей, в том числе APT Groups and Operations [9], Targeted cyberattacks logbook (Лаборатория Касперского) [261], A Threat Actor Encyclopedia (ThaiCERT) [17], Advanced Persistent Threat Groups (FireEye) [18]

Продолжение табл. 2

Тип сведений	Характеристика информационной карты
Модель данных	*Узлы*: «Название APT-группировки» (g), «Средство атаки» (a), «Предполагаемый субъект» (s), «Языковые артефакты» (l), «Жертвы» (v), «Публикация» (so); *Связи*: [g]⇄[g] («Эквивалентность название APT-группировок»), [s]←[g] («Соответствие субъекта и названия APT-группировки»), [g]←[l] («Соответствие языкового артефакта и APT-группировки»), [v]←[g] («Связь жертвы и APT-группировки»), [g]←[a] («Связь APT-группировки и используемого им средства»), [g]←[so] («Связь APT-группировки и источника сведений о нём»), [v]←[so] («Связь жертвы APT-группировки и источника сведений о ней»), [l]←[so] («Связь языкового артефакт APT-группировки и источника сведений о нём»), [s]←[so] («Связь субъекта APT-группировки и источника сведений о нём»), [a]←[so] («Связь средства атаки и источника сведений о нём»); *Свойства*: «Название» (g, a, s, l, v, so), «Описание» (g, a, s, l, v), «Доменное имя» (so), «URL-адрес» (so)
Операции построения	В ходе построения карты осуществлены следующие операции: - автоматизированный сбор сведений из [7, 8, 15, 16, 9, 19, 17, 18] и внесении их в СУБД Neo4j; - построение графов связей ([g]⇄[g]) и ([g]⇄[g], [s]←[g], [g]←[l], [g]←[a]) для соответствующих проекций; - укладка графов в двухмерном пространстве с помощью силового алгоритма ForceAtlas2 (LinLog = true, «Влияние весов рёбер» = 1, «Запрет перекрытия» = true, «Устойчивость» = 1, Theta = 1.2, «Разрежённость» = 1, «Гравитация» = 1); - построение тепловой карты на основании графа связей («Радиус»=0.02, «Распределение пикселей»=0,001); - формирование слоёв объектов исследований в результате отбора соответствующих данных и применения методов (п. 5.1.2.3)
Ландшафты	*Проекция «APT_g_g»*: сетевой ландшафт (на основе связей [g]⇄[g]). Проекция использована для выявления кластеров названий APT-группировок. *Проекция «APT_g_s_a_l»:* - сетевой ландшафт (на основе связей [g]⇄[g], [s]←[g], [g]←[l], [g]←[a]); - тепловая карта на основе сетевого ландшафта
Слои	Слои объектов исследования включают: - области расположения предполагаемых субъектов («Серая зона», «Запад», «Криминал», «Арабские страны», «Китай», «Россия», «Иран», «Северная Корея»); - кластеры названий APT-группировок; - источники сведений об APT-группировках («Лаборатория Касперского», «FireEye», «ATT&CKv9», «APTMAP», «APT Groups and Operations», «ThaiCERT»); - объекты атаки («Государственный сектор», «Финансовый сектор», «Промышленный сектор») и др.
Форматы карты	.qgz (карта для программы QGIS), .gephi (графы для программы Gephi), .zip (дамп базы данных Neo4j)
Автор	Сердечный А.Л.

Общий план информационной карты «APT-группировки» для проекции «APT_g_s_a_l» показан на рис. 2.

Зоны расположения предполагаемых APT-группировок, показанные на рис. 2, определены на основании сведений о принадлежности группировки к той или иной стране. Такие сведения получены в основном на основании публикаций западных исследователей, а проверка их достоверности не представляется возможной ввиду отсутствия информации об использованных методах атрибуции соответствующих APT-группировок. В «Серой зоне» представлены названия групп, которые в основном используют общедоступные средства, а спектр их целей разнообразен. Эти особенности делают задачу атрибуции таких групп крайне сложной.

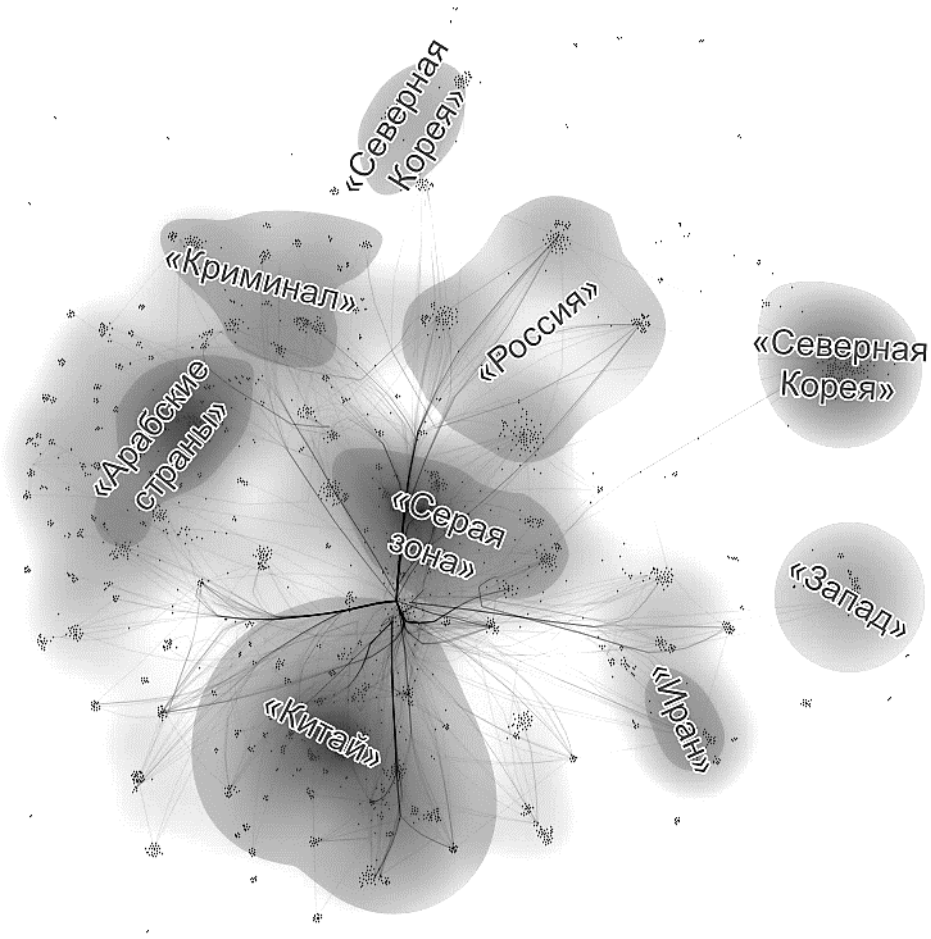

Рис. 2. Общий план информационной карты «APT-группировки»
(проекция «APT_g_s_a_l»)

Отдельно необходимо отметить кластер «Криминал», в котором по большей части представлены названия и средства APT-группировок, атакующие финансовый и промышленный сектор. Как правило, такие группировки имеют интернациональный состав и преследуют цели личного обогащения. Зона «Северная Корея» представлен двумя областями, одна из которых расположена недалеко от кластера «Криминал».

Как было сказано ранее, каждый из исследователей самостоятельно определяет имя APT-группировки, поэтому возникает ситуация, когда одному и тому же субъекту приписываются разные названия. Для того, чтобы определить состав уникальных субъектов, упоминаемых в рассмотренных источников, была составлена карта связей названий, используемых различными источниками (рис. 3).

В результате кластеризации данного графа выделены 155 кластеров, каждый из которых соответствовал изолированной компоненте за исключением двух кластеров, отмеченных в центре карты. Эти группы состоят из 2 и 6 кластеров соответственно. Данные кластеры в рамках исследований рассматривались как уникальные субъекты. Название кластера определялось на основании двух наиболее влиятельных узлов (в качестве метрики влияния узла был использован показатель PageRank)

В проекции «APT_g_s_a_l» (рис. 4, 5) каждый такой кластер показан в виде одной или двух меток. Две метки ставились, если кластер в новой проекции разделялся на две части (например, кластер «lazarusgroup (silentcholima)», рис. 4).

Рис. 3. Общий план информационной карты «APT-группировки»
(проекция «APT_g_g»)

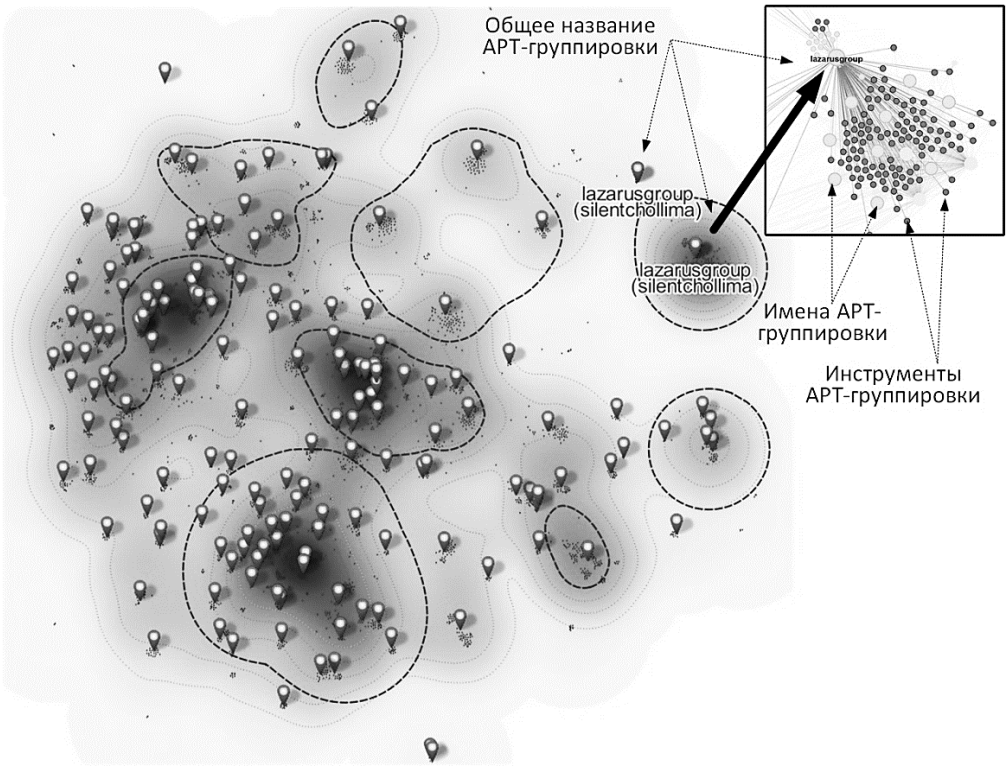

Рис. 4. Общий план информационной карты «APT-группировки» с нанесёнными на неё метками кластеров названий APT-группировки (проекция «APT_g_s_a_l»)

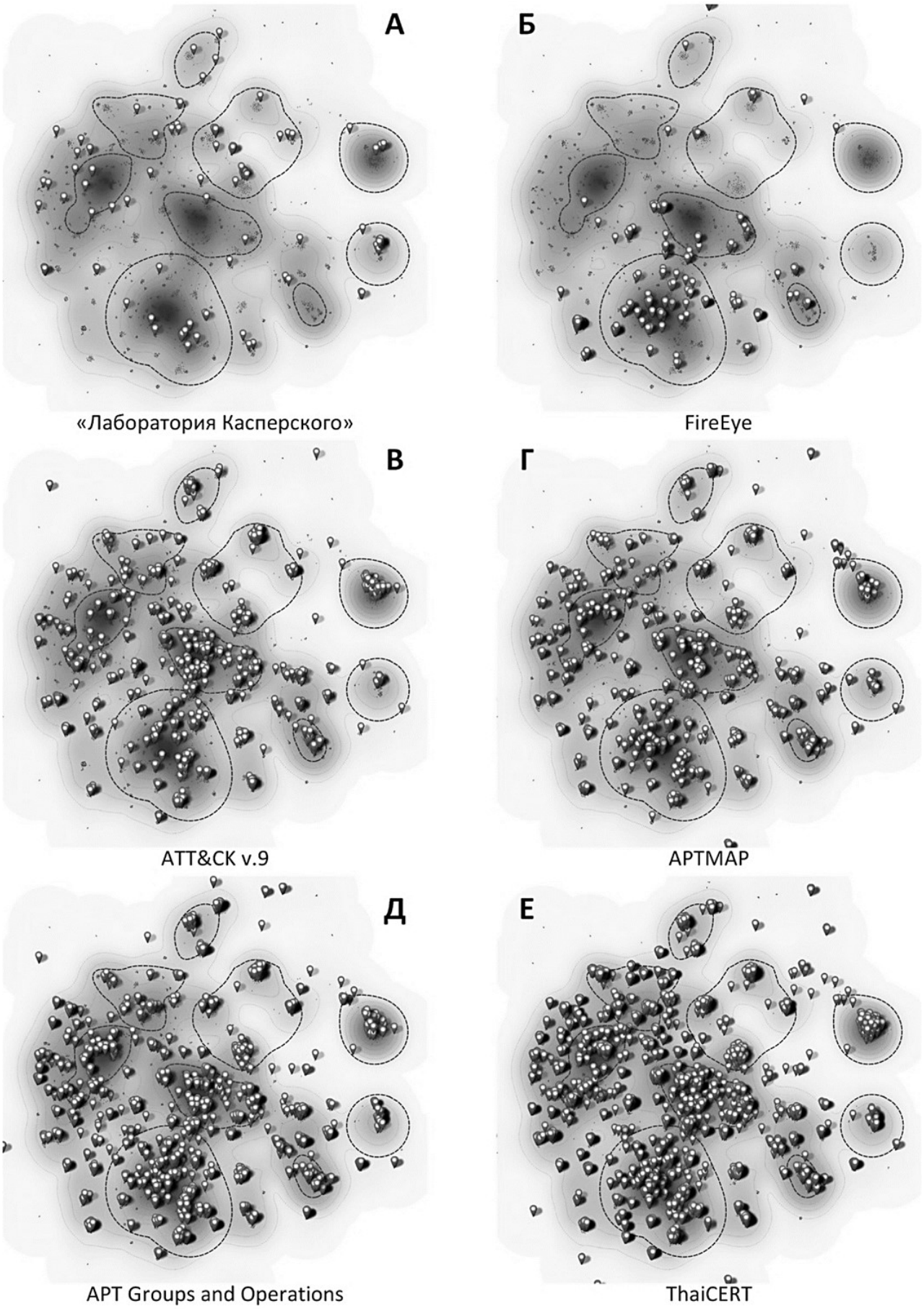

Рис. 5. Названия группировок, упоминаемые в источниках [7, 9, 15, 17, 18, 19], нанесённые на карту «APT-группировки» (проекция «APT_g_s_a_l»)

Меньше всего различных названий APT-группировок упоминается в источниках [18, 19]. Эти источники содержатся лишь те сведения, которые были получены в ходе собственных исследований вредоносного программного обеспечения. При этом необходимо отметить, что «Лаборатория Касперского» отражает практически все крупные APT-группировки, а FireEye акцентирует внимание лишь на зонах «Китай» и «Иран». Для зон «Запад», «Арабские страны» и «Криминал» присутствует всего лишь одно название [18].

Остальные четыре источника являются агрегаторами сведений об APT-группировках, поэтому в них представлено наибольшее число названий. Судя по карте, источник [17] является наиболее полным из всех.

Аналогичным образом можно провести анализ полноты и направленности отчётов о результатах исследований вредоносного программного обеспечения, на которые имеются ссылки в рассмотренных источниках. Использование других проекций, например, в которых основой ландшафта информационной карты являются не APT-группировки, а объекты защиты, дают другой взгляд на деятельность субъектов.

В настоящей работе был показан лишь один из примеров реализации картографического подхода к анализу угроз безопасности информации. Информационные карты могут таким же образом визуализировать в режиме реального времени сведения о компьютерных атаках, что обеспечивает лучшую осведомлённость о текущей ситуации и позволяет более эффективно оказывать противодействие существующим угрозам.

Противодействие киберпреступности

Современные информационные технологии (такие как децентрализованные анонимные сети и Blockchain) выводят компьютерную преступность на новый уровень организации, позволяя ей автономно существовать в виртуальном пространстве без национальных, культурных, пространственных, технологических и финансовых ограничений. Если раньше виртуальное пространство позволяло киберпреступникам обеспечивать только лишь координацию своих действий в рамках разработки вредоносного программного обеспечения, то с развитием Blockchain-технологий ей стала доступна возможность анонимного ведения финансовой деятельности. Это привело к усложнению внутренней структуры киберпреступных группировок и появлению новых форм специализации преступной деятельности. Киберпреступность стала одной из самых опасных угроз для технически развитых стран, получив технические возможности, ранее доступные лишь ведущим государствам.

В настоящий момент противодействие компьютерной киберпреступности осуществляется по следующим направлениям:

- повышение защищённости информационных систем;
- раскрытие личности и арест киберпреступников;
- борьба с вредоносным программным обеспечением;
- выявление и ликвидация информационной инфраструктуры злоумышленников (ботнетов, сайтов, telegram-каналов, торговых онлайн-площадок и др.);
- выявление и анализ финансовых потоков киберпреступности.

Использование картографического подхода позволяет повысить эффективность противодействия на каждом направлении. Примеры задач противодействия компьютерной преступности, решаемых с использованием информационных карт, представлены в табл. 3.

Одним из таких направлений является проведение анализа финансовых операций злоумышленников. Как было сказано ранее, появление технологии Blockchain предоставило киберпреступникам возможности ведения финансовой деятельности в виртуальном пространстве за счёт использования криптовалют.

Таблица 3

Примеры задач обеспечения противодействия компьютерной преступности, решаемых с использованием информационных карт

Задача информационной картографии	Задача противодействия компьютерной преступности
Разведка	
Исследование неизведанных территорий	Выявление новых классов киберпреступности
Выявление скрытых структур и элементов	Выявление цифровых следов киберпреступников, картографическая форензика (компьютерная экспертиза с помощью информационно-картогарфических систем)
Выявление противоборствующих сторон	Определение состава киберпреступных группировок
Планирование операций	
Анализ ресурсов противоборствующих сторон	Определение возможностей киберпреступных группировок
Прокладка маршрута	Определение характеристик средств киберпреступных группировок
Прогнозирование обстановки	Оценка уровня киберпреступности, мониторинга Blockchain и Даркнет
Мониторинг обстановки	
Координация взаимодействия	Реагирование на инциденты
Выявление изменений обстановки	Выявление изменений состава и возможностей киберпреступников, мониторинга Blockchain и Даркнет
Выявление ошибок и дезинформации	Обнаружение противоречий между различными источниками сведений о киберпреступных группировках, выявление атак «под чужим флагом», оценка эффективности ложных информационных систем
Представление знаний	
Обучение	Обучающие информационные карты по мерам защиты от компьютерных атак, визуализация киберучений и соревнований «Захват флага» (Capture the Flag)
Структурированное хранение знаний	Ведение баз данных, используемых при расследовании компьютерных преступлений
Картографический поиск информации	Выявление новых источников сведений о методах, способах и средствах реализации компьютерных атак

Важной особенностью криптовалют, построенных на основе Blockchain, является открытость базы данных совершаемых транзакций. Она позволяет отследить маршруты передачи средств, с другой, из-за большого объёма данных, а также наличия механизмов анонимизации даёт некоторые возможности сокрытия личности отправителя и получателя.

Так, например, для криптовалюты Bitcoin существует механизм запутывания следов, названный «миксером» [20]. Данный механизм за счёт порождения большого количества транзакций, отправляемых с одного кошелька на другой, скрывает суммы и субъекты финансовых операций. Подобно тому, как заяц запутывает след, бегая между деверьями, «миксер» смешивает для внешнего наблюдателя все полученные криптомонеты в единую «петлю», фиксируя, при этом, во внутренней базе данных информацию о всех генерируемых транзакциях. Однако, в аналогии с заячьим следом, если подняться над лесом, то можно различить след при входе в «петлю» и выходе из неё. Точно также видны все транзакции, входящие в «миксер» и исходящие из него.

Другим важным субъектом Blockchain-взаимодействий являются криптовалютные биржи. С помощью них происходит обмен криптовалюты на реальные активы, что позволяет киберпреступникам обналичивать виртуальные деньги.

Для возможности проведения анализа киберпреступной финансовой деятельности требуется постоянный мониторинг

совершаемых Blockchain-транзакций и определение принадлежности криптокошельков различным субъектам. Существует ряд исследований [20, 21, 22, 23, 25, 26], в которых используются методы анализа и визуализации графов для задач анализа Bitcoin-транзакций. При подготовке настоящей работы также проводились подобные исследования, где этом в отличии от рассмотренных работ, помимо анализа транзакций криптовалют Bitcoin, осуществлены аналогичные исследования для криптовалюты Ethereum.

На рис. 6 приведены изображения типовых участников Bitcoin-транзакций, полученные с помощью разработанной системы картографирования рисков защищаемого киберпространства.

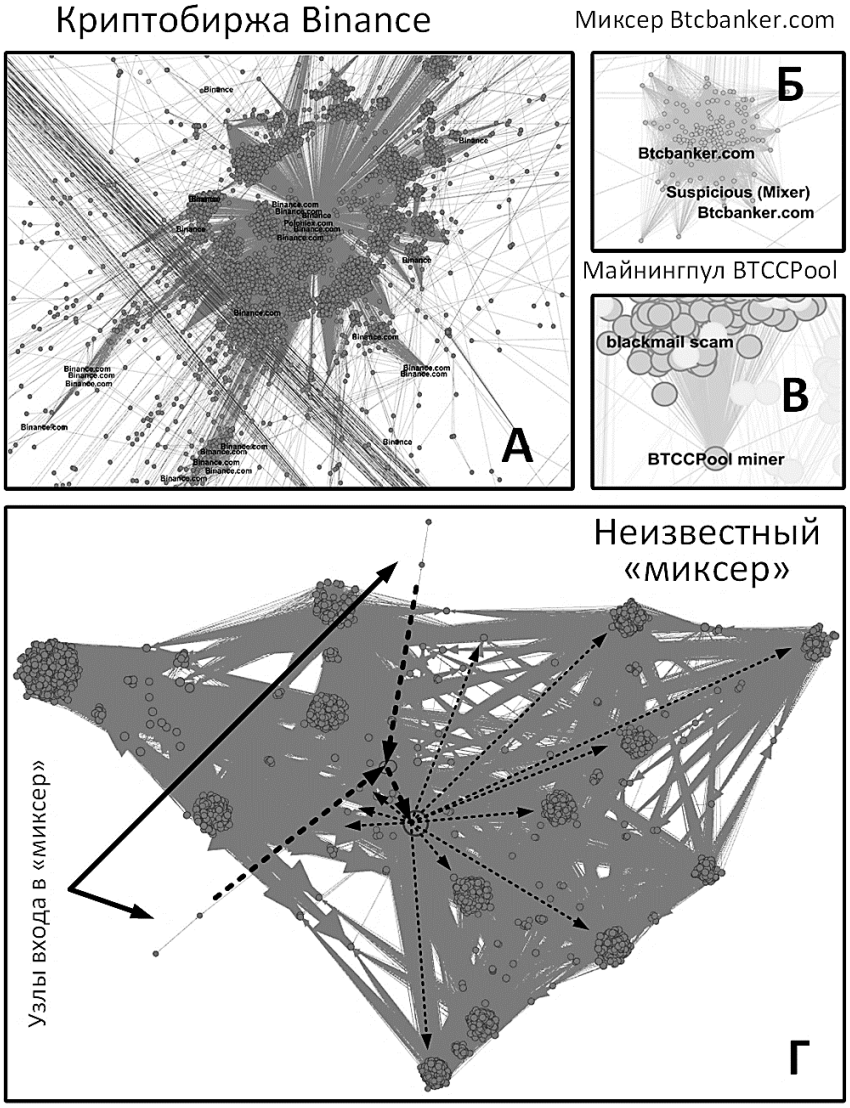

Рис. 6. Изображения участников Bitcoin-транзакций с помощью графа связей криптокошельков (А – одна из наиболее крупных криптобирж Binance, Б – «миксер» Btcbanker, В – майнингпул BTCCPool, Г – неизвестный «миксер»)

Изображения основаны на графе транзакций, сведения о которых собраны за 3 часа работы сети Bitcoin (блок с транзакциями формируется каждые 10 минут).

Самым заметным объектом за наблюдаемый период оказалась криптобиржа Binance (рис. 6 А), которая основана в 2017 году в Гонконге и в настоящий момент является одной из самых крупных международных онлайн-сервисов обмена цифровых валют. Её услугами нередко пользуются киберпреступники для перевода криптовалюты в реальные активы. Для определения криптокошельков, относящихся к данному объекту, были использованы дополнительные информационные ресурсы (WalletExplorer [27] и Vivigle [28]).

В общем потоке транзакций наиболее просто выявляются майнинг-пулы (рис. 6 Б). Майнинг-пулом называется специальный

сервер, который используется для того, чтобы объединять вычислительные ресурсы нескольких участников, для «добычи» криптовалюты (или других цифровых активов). Сведения о них можно обнаружить путём отслеживания первой транзакции создаваемых блоков криптовалют. Также необходимо отметить, один из кошельков майнинг-пула, показанного на рис. 6 Б, был помечен как «blackmail scram». Данная метка установлена на основании сведений базы данных BitcoinAbuse [29], в которой каждый желающий может оставить информацию о подозрительных Bitcoin-кошельках. Помеченный кошелёк принадлежал злоумышленнику, который заражал компьютеры жертв с целью подмены адресатов для всех совершаемых ими Bitcoin-транзакций. При каждом переводе жертвы сумма попадала на счёт киберпреступника. По всей видимости, один из компьютеров майнинг-пула был заражён этой программой.

Ресурсы, подобные базе данных BitcoinAbuse, важны для выявления финансовой инфраструктуры киберпреступных сообществ. В результате возросшей активности криптовымогателей [26] перечень ресурсов о цифровых кошельках пополнился базой данных Ransomwhere [30].

Наиболее важным с точки зрения отслеживания киберпреступников является наблюдение за «миксерами». Изображения двух различных «миксеров» показаны на рис. 6 В и 6 Г. Все транзакции, связанные с подобными структурами, должны вызывать особое внимание. Подобные структуры порождают большое количество новых криптокошельков, что затрудняет анализ данных. В зависимости от алгоритма генерирования транзакций, использование аналитических методов выявления узлов «миксеров» может быть затруднено, однако, картографический способ разметки упрощает этот процесс. Кроме того, при наличии возможностей многопользовательского картографирования, процедура разметки криптокошельков может быть масштабирована пропорционально количеству аналитиков.

Таким образом, рассмотренный пример противодействия компьютерной преступности за счёт визуального анализа Blockchain-транзакций подтверждает необходимость использования информационно-картографических систем для противодействия киберпреступности. Данные системы не только предоставляют наглядные средства мониторинга за активностью подозрительных сообществ, но и повышают эффективность аналитических возможностей исследователей, в том числе за счёт организации совместной обработки данных. При этом, использование методологии информационного картографирования не ограничивается лишь этой задачей.

Анализ вредоносного программного обеспечения как инструмента кибератак

Анализ вредоносного программного обеспечения является одним из базовых элементов для решения более сложных задач противодействия APT-угрозам и киберпреступности, рассмотренных ранее. Без разбора механизмов работы вирусов, троянов и эксплойтов невозможно атрибутировать APT-группировку или разработать правила обнаружения вредоносных средств злоумышленников.

Технологии открытого кода и совместной разработки программного обеспечения в руках киберпреступности на порядки повышают их эффективность, позволяя создавать с каждым разом всё более совершенные средства нападения. Использование подобных методов по уровню потенциала приблизило киберпреступность к возможностям киберподразделений государств.

Вместе с тем не стоят на месте и методы защиты от угроз нарушения безопасности информации. Технологии машинного обучения используются для автоматической классификации вредоносных программ [31], создаются общедоступные экспертные системы и базы знаний о вредоносных программах (например, VirusTotal [32]), формируя тем самым платформу для исследователей в области защиты информации.

В условиях колоссального роста сведений о вредоносном программном обеспечении требуется применение особых подходов к их анализу. Информационные карты являются одним из перспективных направлений и уже активно внедряются в

процесс исследований. Так, например, информационный ресурс VirusTotal, имеет удобный инструмент работы со связанными данными – VT Graph [33]. VT Graph представляет собой веб-приложение для визуальной работы с базой данных VirusTotal в виде графа элементов, таких как «Файл», «Доменное имя», «IP-адрес» и др. (рис. 7), но возможности VT Graph ориентированы лишь на небольшие графы.

В определённой степени VT Graph можно рассматривать в качестве подобия информационно-картографической системы для работы с информационными картами крупного масштаба.

Объединение сведений в рамках единого визуального пространства способствует выявлению закономерностей, присущих исследуемому образцу. Некоторые примеры задач анализа вредоносных программ, решаемых с использованием информационных карт, представлены в табл. 4.

Рис. 7. Граф связей, построенный для криптовымогателя WannaCry с помощью VT Graph [33]

Таблица 4

Примеры задач анализа вредоносных программ, решаемых с использованием информационных карт

Задача информационной картографии	Задача противодействия компьютерной преступности
Разведка	
Исследование неизведанных территорий	Выявление новых классов вредоносных программ, выявление новых способов компьютерных атак
Выявление скрытых структур и элементов	Выявление семейств вредоносных программ
Выявление противоборствующих сторон	Генеалогия вредоносных программ, исследование способов компьютерных атак
Планирование операций	
Анализ ресурсов противоборствующих сторон	Оценка характеристик вредоносных программ
Прокладка маршрута	Определение скорости разработки вредоносных программ, определение времени реализации компьютерной атаки
Прогнозирование обстановки	Прогнозирование эпидемий компьютерных вирусов, прогнозирование развития компьютерной атаки, разработка мер защиты от компьютерных атак
Координация взаимодействия	Обмен сведениями о вредоносных программах
Выявление изменений обстановки	Выявление активности семейств вредоносных программ
Мониторинг обстановки	
Выявление ошибок и дезинформации	Определение авторства вредоносных программ, исследование антиотладочных механизмов, обнаружение противоречий между различными источниками сведений о вредоносных программах
Представление знаний	
Обучение	Разработка информационных карт по реверсинжинирингу (обратной разработке), изучение способов реализации компьютерных атак
Структурированное хранение знаний	Ведение баз данных семейств вредоносных программ и способов реализации компьютерных атак, представление онтологии объектов защиты
Картографический поиск информации	Выявление сведений о новых методах, способах и средствах реверсинжиниринга

На основе результатов анализа вредоносных программ могут быть выявлены сведения как об их разработчиках, так и преступных группировках, которые используют такие средства. Для этого вирусные аналитики определяют общие структурные и поведенческие признаки обнаруженных средств осуществления компьютерных атак. Обобщение этих признаков позволяет установить типовые способы совершения компьютерных атак, присущие конкретным злоумышленникам.

Текущие результаты анализа публикуются в отчётах антивирусных лабораторий и включаются в специализированные базы данных типа ATT&CK [7], MISP [8], рассмотренные ранее.

Анализ связей способов осуществления компьютерных атак с киберпреступными группировками позволяет спуститься на уровень ниже (от состава субъектов кибервойны к особенностям поведения конкретных представителей). Для демонстрации этого используем информационную карту, построенную на основании сведений онтологии D3FEND [34]. Сведения о разработанной информационной карте представлены в табл. 5, а сама карта изображена на рис. 8.

Каждый способ связан с объектом воздействия, а объекты между собой по принципу «часть-целое». Расположение объектов определяет разметку ландшафта карты.

Таблица 5

Сведения об информационной карте «D3FEND»

Тип сведений	Характеристика информационной карты
Уровень	Уровень объектов защиты, относящийся к информационному уровню киберпространства
Решаемые задачи	Исследование неизведанных территорий, выявление противоборствующих сторон, прокладка маршрута, прогнозирование обстановки, обучение, структурированное хранение знаний, картографический поиск информации
Исходные данные	Онтология D3FEND [34].
Модель данных	*Узлы*: «Класс способов» (ca), «Способ атаки» (a), «Объект» (o), «Группа мер защиты» (cd), «Мера защиты» (d), «Источник» (so); *Связи*: [ca]←[a] («Принадлежность способа определённому классу»), [o]⇄[o] («Связь между объектами»), [o]←[a] («Связь атаки с атакуемым объектом»), [cd]←[d] («Принадлежность меры группе мер»), [o]←[d] («Связь меры с объектом защиты»), [a]←[so] («Связь способа атаки и источника, в котором она описана), [o]←[so] («Связь объекта и источника сведений о ней»), [d]←[so] («Связь меры защиты и источника сведений о ней»); *Свойства*: «Название» (ca, a, o, cd, d, so), «Описание» (ca, a, o, cd, d), «Доменное имя» (so), «URL-адрес» (so)
Операции построения	В ходе построения карты осуществлены следующие операции: - загрузка онтологии [34] в СУБД Neo4j с помощью модуля Neosemantics; - построение графа связей ([o]⇄[o], [o]←[a] и [o]←[d]); - 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» = 2, «Гравитация» = 1); - построение полигона на основании графа связей (тепловая карта с параметрами «Радиус»=0.02, «Распределение пикселей»=0,001, изолиния с плотностью точке = 1); - формирование слоёв объектов исследований в результате отбора соответствующих данных и применения методов (п. 5.1.2.3), а также совмещения со сведениями об APT-группировках из соответствующей информационной карты (табл. 2)
Ландшафты	*Проекция «D3FEND_a_d_o»*: - сетевой ландшафт (на основе связей [o]⇄[o], [o]←[a], [o]←[d]); - полигон на основании тепловой карты сетевого ландшафта
Слои	Слои объектов исследования включают: - области типов объектов; - классы реализации компьютерных атак; - APT-группировка «Equation» и др.
Форматы карты	.qgz (карта для программы QGIS), .gephi (графы для программы Gephi)
Автор	Сердечный А.Л.

Основная часть способов сконцентрирована в центре карты и связана с повышением привилегий внутри операционной системы. В правой части расположены способы реализации сетевых атак. С высокоуровневыми объектами (такими как «Сервер», «Облачное хранилище», «Информационная система»), которые расположены на изолированном «острове» (рис. 8), с которым не связан ни один из способов.

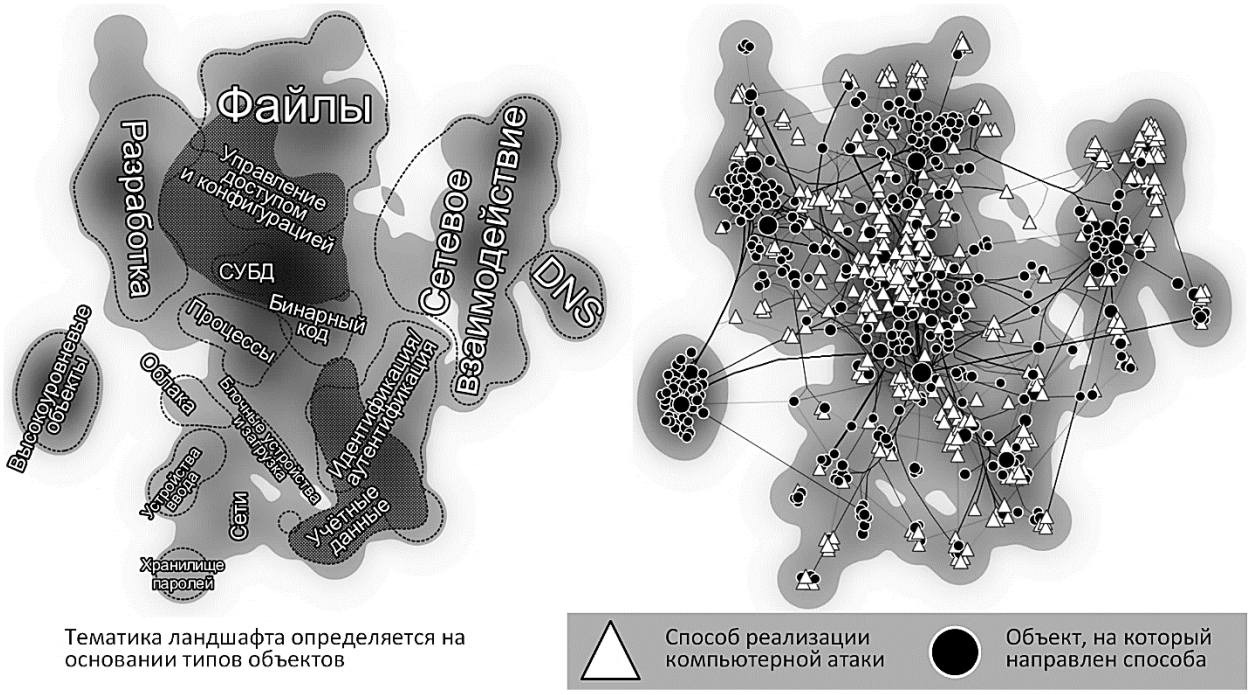

Рис. 8. Информационная карта связей способов реализации компьютерных атак и объектов воздействия, построенная на основании онтологии D3EFENS [34]

Данную карту удобно использовать для исследования и демонстрации отличий киберпреступных группировок. На рис. 9 показаны способы реализации компьютерных атак, использованные группировкой Equation [35].

Для обозначения способов использованы идентификаторы технических приёмов матрицы ATT&CK [7]. Глядя на карту можно установить, что группировка Equation в меньшей степени использует способы, связанные с воздействием на файлы. Данное обстоятельство может быть обусловлено как спецификой поведения самой группировки, так и недостаточной полнотой источников данных о ней. При этом опытным путём установлено, что наблюдая всю картину целиком, и имея возможность интерактивного взаимодействия с картой, исследователю гораздо проще выявить особенности поведения группировок, нежели на основании анализа текстовой информации или традиционных диаграмм. При должном опыте и знании разметки, ему достаточно одного взгляда на изображение, чтобы установить все ключевые детали. В текстовом виде пришлось бы вчитаться в страницы отчёта, что занимает гораздо больше времени и не гарантирует успех аналитики.

Таким образом, в настоящей работе показано, что информационные карты можно использовать в качестве инструмента решения различных задач в области защиты информации. Были рассмотрены различные примеры, связанные с визуализацией деятельности киберпреступных группировок. Перспективным направлением исследований в данной области видится использование информационных карт для исследования защищённости информационных систем, мониторинга и обнаружения компьютерных атак и разработки безопасного программного обеспечения (выявления уязвимостей программного обеспечения).

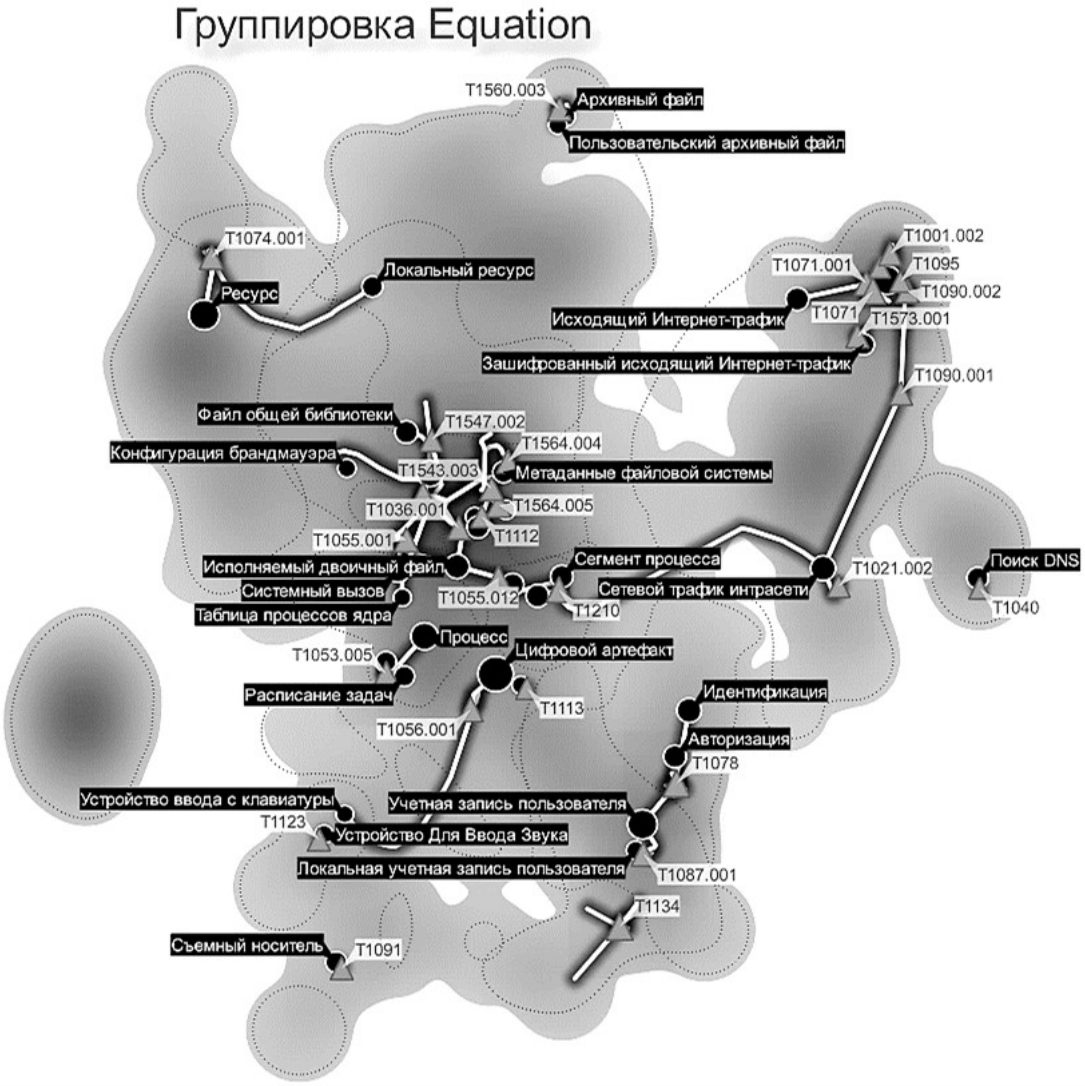

Рис. 9. Информационная карта, отражающая способы реализации компьютерных атак, использованные APT-группировкой Equation [35]

Список литературы

1. Endsley M.R. Toward a theory of situation awareness in dynamic systems / M. R. Endsley // Human factors. 1995. Т. 37. №. 1. С. 32-64.

2. Franke U. Cyber situational awareness–a systematic review of the literature / U. Franke, J. Brynielsson // Computers & security. 2014. Т. 46. С. 18-31.

3. Ситуационный центр управления кибербезопасностью. URL: https://legion-project.ru/solutions/situation-centr-cybersecurity/ (дата обращения 07.09.2021).

4. Corneille O. Threat and the group attribution error: When threat elicits judgments of extremity and homogeneity / O. Corneille, V. Y. Yzerbyt, A. Rogier и др. // Personality and Social Psychology Bulletin. 2001. Т. 27. №. 4. С. 437-446.

5. Raff E. Automatic YARA rule generation using biclustering / E. Raff, R. Zak, G. Lopez Munoz и др. // Proceedings of the 13th ACM Workshop on Artificial Intelligence and Security. 2020. С. 71-82.

6. YARA // URL: https://github.com/VirusTotal/yara (дата обращения 07.09.2021).

7. Онтология ATT&CK // URL: https://attack.mitre.org (дата обращения 07.09.2021).

8. Методология MISP // URL: https://www.misp-project.org/ (дата обращения 07.09.2021).

9. APT Groups and Operations - Google Drive // URL: https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit (дата обращения 07.09.2021).

10. Gray J. Identifying Authorship Style in Malicious Binaries: Techniques, Challenges & Datasets / J. Gray, D. Sgandurra, L. Cavallaro //

arXiv preprint arXiv:2101.06124. 2021. С. 1-31.

11. APT & Cybercriminals Campaign Collection // URL: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections (дата обращения 07.09.2021).

12. Mapping the Connections Inside Russia's APT Ecosystem // URL: https://www.intezer.com/blog/malware-analysis/russian-apt-ecosystem/ (дата обращения 07.09.2021).

13. Meng X. Identifying multiple authors in a binary program / X. Meng, B. P. Miller, K. S. Jun // European Symposium on Research in Computer Security. Springer, Cham, 2017. С. 286-304.

14. Meng X. Binary code multi-author identification in multi-toolchain scenarios / X. Meng, B. P. Miller // Under Submission. 2018. С. 1-15.

15. Threat Actor Map // URL: https://aptmap.netlify.app/ (дата обращения 07.09.2021).

16. Malpedia // URL: https://malpedia.caad.fkie.fraunhofer.de/actors (дата обращения 07.09.2021).

17. A Threat Actor Encyclopedia // URL: https://apt.thaicert.or.th/cgi-bin/listgroups.cgi (дата обращения 07.09.2021).

18. Advanced Persistent Threat Groups // URL: https://www.fireeye.com/current-threats/apt-groups.html (дата обращения 07.09.2021).

19. Targeted cyberattacks logbook // URL: https://apt.securelist.com/ (дата обращения 07.09.2021).

20. Zhang H. A Survey of the Dark Web and Dark Market Research / H. Zhang, F. Zou // 2020 IEEE 6th International Conference on Computer and Communications (ICCC). IEEE, 2020. С. 1694-1705.

21. Dupuis D. Money laundering with cryptocurrency: open doors and the regulatory dialectic / D. Dupuis, K. Gleason // Journal of Financial Crime. 2020. С. 1-15/\

22. Rastogi S. Visualizing Bitcoin Transactions / Surya Rastogi // Персональный блог на платформе Medium. Дата обновления: 16.03.2018. URL https://medium.com/chainalysis/visualizing-bitcoin-transactions-dd0e67d8e104 (дата обращения 07.09.2021).

23. McGinn D. Visualizing dynamic bitcoin transaction patterns / D. McGinn, D. Birch, D. Akroyd и др. // Big data. 2016. Т. 4. №. 2. С. 109-119.

24. Zhang H. A Survey of the Dark Web and Dark Market Research / H. Zhang, F. Zou // 2020 IEEE 6th International Conference on Computer and Communications (ICCC). IEEE, 2020. С. 1694-1705.

25. Yue X. Bitextract: Interactive visualization for extracting bitcoin exchange intelligence / X. Yue, X. Shu, X. Zhu // IEEE transactions on visualization and computer graphics. 2018. Т. 25. №. 1. С. 162-171.

26. DarkSide Hackers' Bitcoin Stash Tracked // URL: https://finance.yahoo.com/news/darkside-hackers-bitcoin-stash-tracked-202147099.html (дата обращения 07.09.2021).

27. WalletExplorer.com: smart Bitcoin block explore //. URL: https://www.walletexplorer.com/ (дата обращения 07.09.2021).

28. Cryptocurrency wallet rating and analytics – Vivigle // URL: https://vivigle.com/ (дата обращения 07.09.2021).

29. Bitcoin Abuse Database // URL: https://www.bitcoinabuse.com/ (дата обращения 07.09.2021).

30. Ransomwhere // URL: https://ransomwhe.re/ (дата обращения 07.09.2021).

31. Sokolova K. Android application classification and anomaly detection with graph-based permission patterns / K. Sokolova, C. Perez, M. Lemercier // Decision Support Systems. 2017. Т. 93. С. 62-76.

32. VirusTotal // URL: https://www.virustotal.com/gui/ (дата обращения 07.09.2021).

33. VirusTotal Graph // URL: https://www.virustotal.com/graph/ (дата обращения 07.09.2021).

34. D3FEND // URL: https://d3fend.mitre.org/ (дата обращения 07.09.2021).

35. «Звезда Смерти» показалась над горизонтом: APT Equation // URL: https://www.kaspersky.ru/blog/zvezda-smerti-pokazalas-nad-gorizontom-apt-equation/2721/ (дата обращения 07.09.2021).

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 12.09.2021

Информация об авторах

Остапенко Александр Григорьевич – д-р техн. наук, проф., заведующий кафедрой, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Сердечный Алексей Леонидович – канд. техн. наук, старший преподаватель, Воронежский государственный технический университет, e-mail: alex-voronezh@mail.ru

Трубицын Сергей Дмитриевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Нархов Дмитрий Андреевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Остапенко Владимир Юрьевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

CYBERSPACE MAPPING AND INFORMATION PROTECTION

A.G. Ostapenko, A.L. Serdechnyy, S.D. Trubitsyn, D.A. Narkhov, V.Yu. Ostapenko

The article discusses the provision of situational awareness of information security threats and computer attacks using incident response centers and information maps, including situational cybersecurity control centers. The aforementioned awareness is illustrated by information maps of the ART groups, reflecting: the composition of the victims and those interested in them in the attack of strings; artifacts in the code of malicious software; attribution of a grouping based on the author's style of writing software for implementing computer attacks. In this regard, general plans of information cards for various ART groups are presented. At the same time, countering cybercrime using information cards is discussed. The analysis of financial transactions of cybercriminals in the virtual space through the use of cryptocurrencies is discussed. Using the examples of Blockchain and Bitcoin transactions, he considers the determination of the ownership of crypto wallets. With the help of a link graph, the above transactions are illustrated. Analysis of malware as a cyber attack tool is also proposed. In this regard, an information map of connections between methods of implementing computer attacks and objects of influence, built on the basis of an ontology, is considered.

Keywords: situational awareness, information map, cybersecurity, cryptocurrency, transactions.

Submitted 12.09.2021

Information about the authors

Alexander G. Ostapenko – Dr. Sc. (Technical), Head of Department, Voronezh State Technical University, e-mail: mnac@comch.ru

Alexey L. Serdechnyy – Cand. Sc. (Technical), Senior Lecturer, Voronezh State Technical University, e-mail: alex-voronezh@mail.ru

Sergey D. Trubitsyn – Student, Voronezh State Technical University, e-mail: mnac@comch.ru

Dmitriy A. Narkhov – Student, Voronezh State Technical University, e-mail: mnac@comch.ru

Vladimir Yu. Ostapenko – Student, Voronezh State Technical University, e-mail: mnac@comch.ru