АНАЛИЗ МОДЕЛЕЙ И МЕТОДИК, ИСПОЛЬЗУЕМЫХ ДЛЯ АТРИБУЦИИ НАРУШИТЕЛЕЙ КИБЕРБЕЗОПАСНОСТИ ПРИ РЕАЛИЗАЦИИ ЦЕЛЕВЫХ АТАК

Котенко И.В.[1], Хмыров С.С.[2]

Цель работы: *анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности в интересах построения перспективной системы атрибуции при реализации целевых атак на объекты критической информационной инфраструктуры.*

Метод исследования: *системный анализ открытых источников данных по атрибуции кибернарушителей при реализации целевых атак на объекты критической информационной инфраструктуры за период в основном за последние пять лет.*

Полученный результат: *на базе рассмотрения открытых источников в работе представлен анализ моделей и методик, используемых для атрибуции кибернарушителей при реализации целевых атак, и применяемых как в научных, так и практических проектах. В работе проведен анализ новых моделей, используемых для атрибуции, позволяющих осуществлять сбор данных на тактико-техническом и социо-политическом уровнях. Выделены основные показатели проводимых кибератак и нарушителей, существенные для реализации процессов атрибуции. Рассмотрен порядок формирования данных для профилирования кибергруппировок, а также возможности применения рассмотренных моделей и методик в интересах построения перспективной системы атрибуции кибернарушителя при реализации целевых атак на объекты критической информационной инфраструктуры. Анализ выполнен по источникам за двадцатилетний период, между тем основные рассматриваемые работы были опубликованы за последние пять лет. Анализ не претендует на полноту, но делается попытка охватить наиболее значимые исследования.*

Научная новизна *состоит в том, что представленная статья является одной из первых отечественных работ, предоставляющих развернутый анализ исследований, опубликованных за последние годы в области атрибуции нарушителей кибербезопасности. Рассмотрены такие модели как «цепочка кибервторжений», «унифицированная цепочка кибервторжений», базовая и расширенная модели анализа вторжений Diamond, модель ATT&CK. Приведены примеры методик атрибуции - аргументированного рассуждения с доказательствами на техническом и социальных уровнях и использования технических артефактов для выявления ложных флагов при атрибуции. Кроме того, перечислены тенденции в области использования современных решений по обнаружению и атрибуции атак на основе искусственного интеллекта и машинного обучения.*

Ключевые слова: *кибератака, кибероперация, критическая инфраструктура, искусственный интеллект, машинное обучение, продвинутая постоянная угроза, обнаружение вторжений, профилирование нарушителей, цепочка кибервторжений.*

DOI:10.21681/2311-3456-2022-4-52-79

1. Введение

Странами НАТО на саммите 2016 года в Варшаве было признано, что кибератака может причинить ущерб, сопоставимый с ущербом от вооруженного нападения, а киберпространство объявили областью равной другим обычным военным областям — суше, морю и воздуху [1]. Поводом послужили кибератаки, повлиявшие на целостность суверенитета ряда государств [2-6]. По мере того, как технологии становятся все более продвинутыми и сложными, меняются и методики, которые используются в современных кибератаках.

1 Котенко Игорь Витальевич, доктор технических наук, профессор, главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: ivkote@comsec.spb.ru

2 Хмыров Семен Сергеевич, аспирант, ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. E-mail: khmyrov.s.s@gmail.com

Средства защиты информации, применяемые против традиционных угроз безопасности, часто являются неэффективными против современных целевых кибератак. Это связано с тем, что кибернарушители (кибергруппировки), стоящие за вторжением, сосредоточены на конкретной цели и имеют возможность адаптироваться к принятым защитным методам и средствам реагирования на инциденты. Целью нарушителей чаще всего становятся критическая информационная инфраструктура (КИИ) или объекты КИИ. Одним из важнейших инструментов сдерживания государственных агрессий и проведения целенаправленных кибероперациий является способность осуществлять эффективную атрибуцию нарушителя [7, 8], под которой понимается процесс идентификации нарушителя, инициировавшего (реализующего) кибератаку, его целей, мотивов, выполняемых действий и используемых средств реализации атаки.

В большинстве случаев атрибуция нарушителей осуществляется после совершения кибератаки и преимущественно ручным методом. Основу традиционной атрибуции составляет анализ методов и средств, применяемых нарушителями. Возможность эффективной автоматизированной и интеллектуальной атрибуции в реальном времени делает научную задачу исследования и построения эффективных систем атрибуции нарушителей перспективной для исследований.

Для этого необходим развернутый анализ современных моделей, используемых для атрибуции, в интересах построения перспективной системы атрибуции нарушителя при целевых атаках на КИИ.

Работа структурирована следующим образом. Во втором разделе рассматриваются понятия целевых атак и продвинутых постоянных угроз (APT, Advanced Persistent Threats), дается определение понятия атрибуции кибернарушителей, и перечисляются основные проблемы, связанные с созданием систем атрибуции. В третьем разделе проводится анализ моделей, используемых для атрибуции. Во четвертом разделе выполняется предварительный обобщенный анализ подходов к реализации методик и созданию автоматизированных систем атрибуции, а также более детально анализируются две значимых методики, предложенных для атрибуции нарушителей кибербезопасности.

2. Понятия целевых атак, APT и атрибуции

В настоящее время увеличивается количество целевых кибератак на КИИ [9-11]. Однако четкого определения и единых критериев, позволяющих относить разные типы кибератак к целевым, среди экспертов до сих пор не определено [12]. Целевые (таргетированные) кибератаки необходимо отличать от других традиционных кибератак, к которым относятся атаки случайного характера и широкого фокуса, направленные на компрометацию большого количества пользователей и систем. Кибернарушители, осуществляющие целевые кибератаки, четко разделяют цели в ожидании необходимого момента для организации запланированного сценария атаки. У них есть определенные намерения (мотив). В большинстве случаев – это финансовая выгода, нарушение технологических (бизнес) процессов, промышленный шпионаж, кража интеллектуальной собственности, саботаж КИИ. Целевые кибератаки структурированы и технологически продвинуты. Атакующая сторона высоко мотивирована и обладает необходимыми профессиональными навыками. В совокупности данные факторы образуют необходимый базис для целевых кибератак.

Часто целевые кибератаки обозначают как APT (Advanced Persistent Threats) – продвинутые постоянные угрозы [13]. Эксперты утверждают, что целевые кибератаки не всегда носят характер продвинутых постоянных угроз [14]. Отличительная характеристика APT - адаптация к защитным мерам и поиск новых слабых мест в системе безопасности объекта атаки. Как правило, нарушитель обладает значительными ресурсами, которые позволяют ему создавать возможности для достижения целей посредством различных векторов вторжения и оставаться незамеченным в скомпрометированной системе длительное время. Такие кибератаки, по большей части, представляют собой санкционированные правительством специализированные компании, выполняемые преимущественно на информационно-телекоммуникационную инфраструктуру военных и государственных объектов. Чаще всего в проведении целевых вредоносных компаний подозревают спецслужбы других стран и отряды «правительственных хакеров» [15]. Именно такие атаки, которые реализует противник с высоким уровнем знаний и умений, обладающий значительными ресурсами для использования множества различных векторов атак, действующий для достижения некоторой конечной цели, необходимо классифицировать как APT.

Обобщая все сказанное выше, целевые кибератаки – это класс специализированных, многоуровневых атак, направленных на ограниченный и заранее выбранный набор ценных активов или физических систем с явной целью кражи, компрометации конфиденциальных данных или саботажа систем. Данный тип кибератак включает в себя структурированный

комплекс мероприятий, формируя жизненный цикл целевой атаки [16 – 18].

Атрибуция кибератаки – это процесс идентификации происхождения и источника кибератаки с целью установления злоумышленника или группы злоумышленников, инициировавших атаку [19, 20]. Другими словами, под атрибуцией кибератаки понимается процесс установления (определения) субъекта (актора) кибератаки относительно объекта деструктивного воздействия.

Постоянно меняющейся ландшафт киберугроз и стремительный рост экосистемы рынков даркнета [21, 22] позволил применять на практике схожий инструментарий, усложняя идентификацию конкретной кибергруппировки. Методы запутывания аналитиков и аналитических систем во время расследования инцидента также затрудняют атрибуцию. APT стараются подделывать время компиляции, работают в нерабочее время, внедряют различные языки или уникальные культурные свидетельства в строки кода, повторно регистрируют раннее используемые командно-управляющие домены других злоумышленников и т.п.

Применяется универсальное программное обеспечение (ПО), которое эффективно при достижении краткосрочной цели или выполнении узконаправленной задачи. Такое же ПО используют как кибергруппировки, так и отдельные нарушители. Поскольку в большинстве случаев применяется одно и то же ПО, выяснить, стоит ли за целевой кибератакой APT или обычный злоумышленник очень проблематично. Соответственно, свидетельства и доказательства, применяемые для атрибуции атак, можно подделать и замаскировать, тем самым усложнив атрибуцию.

Выделим основные проблемы атрибуции:

- постоянное прогрессирование APT;
- определение источников (мест запуска и инициализации) кибератаки;
- определение ответственного за кибератаку (основного актора);
- обработка большого количества несортированных (сырых) данных;
- децентрализация и запутанность существующих систем публично-частной атрибуции;
- использование методов имитации кибератак с целью формирования ложных обвинений конкретного нарушителя, кибергруппировки и (или) государства;
- APT часто применяют определенные методы и сценарии реализации атаки, выстраивая необходимую среду (экосистему) для достижения поставленных целей, выполняется распределенная согласованная последовательность сложно отслеживаемых этапов (возможно несколько зависимых или независимых цепочек действий).

3. Модели, используемые для атрибуции

3.1. Модель Cyber Kill Chain

Чтобы лучше понимать и анализировать APT была разработана описательная модель Cyber Kill Chain (CKC, «цепочка кибервторжений») и ее расширенная версия. Основой для модели послужила концепция Kill Chain (Цепочки убийств), которая была впервые принята военными для описания действий, используемых противником для атаки и уничтожения цели.

Распознавание этапов CKC дает возможность идентифицировать злоумышленников и принять ответные меры. Используя эту модель, компания Lockheed Martin разработала собственную модель CKC [23].

CKC - это схематическое описание последовательных действий (этапов) нарушителя в виде взаимосвязанных звеньев цепи. Модель направлена на изучение поведения нарушителя.

Базовая версия модели CKC включает в себя (предполагает) семь этапов, необходимых для реализации успешной кибератаки (рис. 1) [24]:

1) разведка;
2) вооружение;
3) доставка;
4) эксплуатация;
5) установка;
6) командование и контроль;
7) выполнение действий.

Модель CKC описывает атаку внешнего злоумышленника, пытающегося получить доступ к данным или активам внутри периметра целевого объекта. Злоумышленник выполняет разведку, вторжение, использование уязвимостей. Далее следует получение и повышение привилегий, перемещение для доступа к более ценным активам. На финальной стадии предпринимается попытка сокрытия своей активности, и производится эксфильтрация (скрытная выгрузка) необходимых данных за пределы целевой среды.

Предлагаемый подход позволяет экспертам идентифицировать методы и средства, применяемые злоумышленниками на каждом этапе кибератаки [25].

Базовая модель неоднократно подвергалась исследователями модернизации для применения в разных областях [26-29], в том числе и для киберфи-

Рис. 1. Этапы базовой модели СКС

зических систем [30]. Традиционная модель СКС ориентирована на учет периметра целевого объекта и использование вредоносного программного обеспечения (ПО). Таким образом, эта модель не охватывает другие векторы атак, происходящие за периметром целевого объекта.

3.2. Модель Unified Kill Chain

С учетом постоянно наращиваемых векторов атак и инструментария нарушителя число этапов было увеличено до 18-ти, и такая модель получила название Unified Kill Chain (UCK, «унифицированная цепочка кибервторжений»). В расширенной версии модели цепочка этапов представлена следующим образом (рис. 2) [31, 32].

Рассмотрим данные этапы.

Этап 1. Разведка (Reconnaissance). На данном этапе, осуществляется сбор информации об атакуемой цели. Устанавливается организационная структура, применяемые информационные технологии, средства защиты (злоумышленники будут пытаться идентифицировать и исследовать существующие межсетевые экраны, системы предотвращения вторжений, механизмы аутентификации и др.). Для выявления «узких» мест и определения наименее защищенных элементов (служб, сервисов) в информационно–коммуникационной инфраструктуре потенциальной жертвы анализируются технологические процессы. В случае с объектами КИИ, проводится возможная

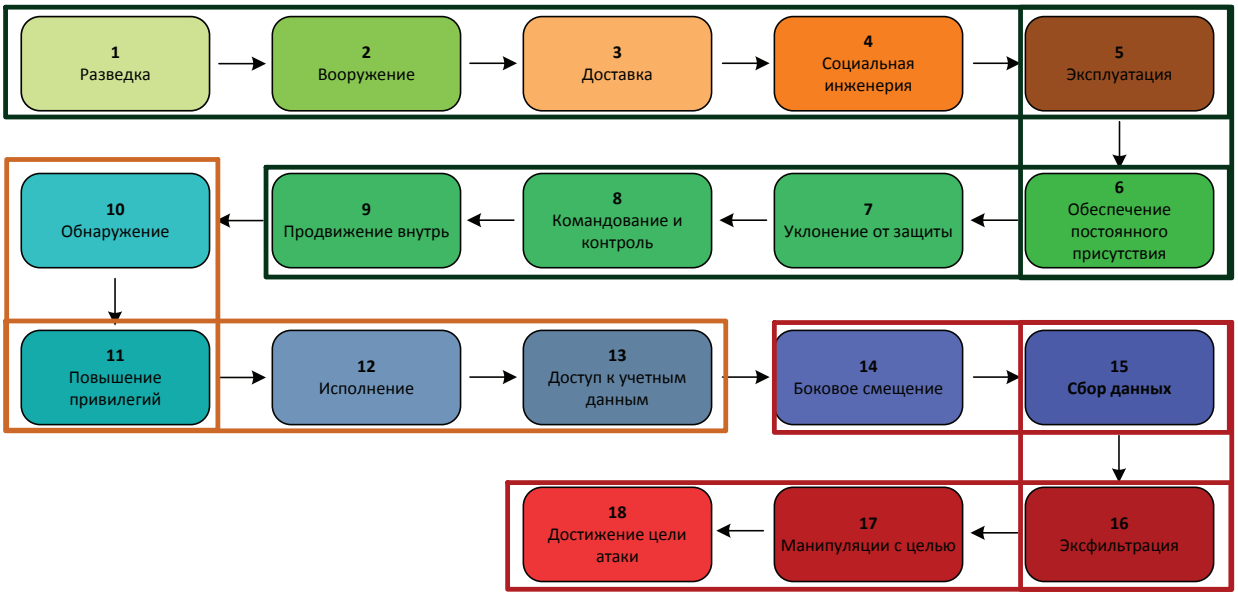

Рис. 2. Этапы расширенной модели UKC

оценка ущерба национальным и стратегическим интересам государства. Полученная информация выступает в роли базы данных и знаний при выполнении следующего этапа.

Этап 2. Вооружение (Weaponization). Выполняются подготовительные мероприятия, направленные на создание инфраструктуры, необходимой для атаки. Используется существующее или разрабатывается собственное уникальное вредоносное ПО, в том числе эксплойты, шифровальщики (ransomware) и т.п.

Этап 3. Доставка (Delivery). Активная фаза атаки, главная задача которой внедрение и распространение применяемого вредоносного решения в целевой среде.

Этап 4. Социальная инженерия (Social Engineering). Применяются методы, направленные на манипулирование персоналом (пользователями) с целью совершения необходимых злоумышленнику (небезопасных) действий.

Этап 5. Эксплуатация (Exploitation). Активация вредоносного решения на скомпрометированном целевом объекте. На этапе эксплуатации злоумышленники ищут дополнительные уязвимости или слабые места, которые они могут использовать в системах организации. Например, извне злоумышленник может не иметь доступа к базам данных, но после вторжения он может увидеть, что база данных использует старую версию ПО и подвержена хорошо известной уязвимости.

Этап 6. Обеспечение постоянного присутствия (Persistence). Осуществляется любой доступ, действие или изменение в доверенной среде с целью обеспечения длительного (постоянного) присутствия злоумышленника в целевой системе.

Этап 7. Уклонение от защиты (Defense Evasion). Применяются методы и средства для обхода средств защиты и сокрытия присутствия в целевой системе.

Этап 8. Командование и контроль (Command & Control). Осуществляется администрирование вредоносного решения, его обновление, получение нового функционала, реализация полного спектра команд для достижения поставленных целей.

Этап 9. Продвижение внутрь (Pivoting). Злоумышленники устанавливают доступ через контролируемую систему в другие системы, к которым нет прямого доступа.

Этап 10. Обнаружение (Discovery). Применяются методы и средства, позволяющие злоумышленнику ориентироваться в системе-жертве для дальнейших действий, получать информацию о целевой системе, сетевом окружении и новых возможностях.

Этап 11. Повышение привилегий (Privilege Escalation). Реализуются методы и средства, которые дают возможность злоумышленнику получить более широкие права в целевой системе. Цель нарушителя - получить привилегии для дополнительных систем или учетных записей. Предпринимаются атаки методом

грубой силы, поиск незащищенных хранилищ учетных данных, осуществляется слежка за незашифрованным сетевым трафиком и т.д.

Этап 12. Исполнение (Execution). Применяются методы и средства, позволяющие выполнять вредоносный код в локальной или удаленной системе.

Этап 13. Доступ к учетным данным (Credential Access). Используются методы и средства, обеспечивающие доступ или контроль над учетными данными системы, службы или домена.

Этап 14. Боковое смещение (Lateral Movement). Используется методика получения нарушителями доступа к другим удаленным системам, подключенным к скомпрометированной целевой среде для управления или деструктивного воздействия, поиска конфиденциальной информации или доступа к критически важным активам. При боковом смещении злоумышленник часто использует уязвимости нулевого дня или конфиденциальные данные из удаленных систем без применения специализированного инструментария.

Этап 15. Сбор данных (Collection). Осуществляются идентификация и сбор необходимых конфиденциальных данных из целевой сети.

Этап 16. Эксфильтрация (Exfiltration). Используются методы и средства скрытной выгрузки данных за пределы целевой среды. Они способствуют краже конфиденциальных данных или удалению данных из целевой сети (попытки замести следы). Эксфильтрация может включать в себя такие методы, как обфускация (например, посредством фальсификации временных меток, удаления или изменения журналов, манипуляции в системе безопасности, чтобы скрыть предыдущие этапы в цепочке уничтожения и создать впечатление, что конфиденциальные данные или системы не были затронуты и т.д.), отказ в обслуживании или шифрование.

Этап 17. Манипуляции с целью атаки (Impact). Реализуются методы и средства манипулирования, прерывания или уничтожения целевой системы и (или) данных (атаки на доступность и целостность) для достижения конечной цели и (или) сокрытия следов.

Этап 18. Достижение цели (Objectives). Выполнение действий по реализации кибератаки, направленных на достижение цели реализации кибератаки.

Модель UKC предполагает, что APT может не пройти все возможные этапы, и некоторые этапы могут повторяться. Например, если на этапе уклонения от защиты нарушитель был обнаружен, последует корректировка применяемых методов с целью прохождения данного этапа до тех пор, пока не будет достигнута цель реализации кибератаки. Повторяющийся набор действий по достижению цели может быть представлен в виде «петли» (рис. 3).

Модель UKC дает понимание сложных кибератак, представляющих собой APT [33-36]. В ходе их реконструкции каждый этап можно разбить на отдельные блоки, характерные для конкретной APT. Блоки могут характеризоваться индивидуальными атрибутами (включая спецификацию поведения, используемых методов и средств).

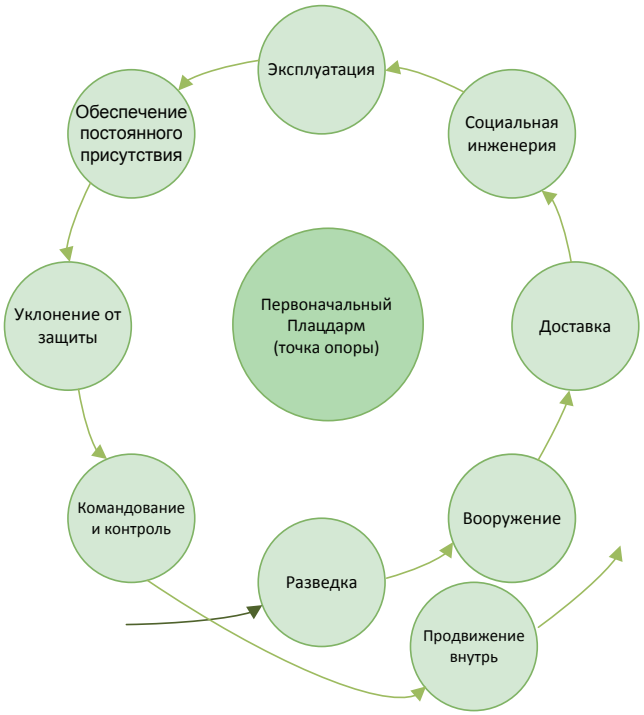

Рис. 3. Представление действий по реализации кибератаки в виде «петли»

С помощью анализа «петли» на отдельных фазах атаки по мере ее реализации можно определить общее количество попыток достижения цели реализации кибератаки. Данная информация позволит сформировать значение атрибутов «Настойчивость» или «Интенсивность», характеризующих нарушителя (или APT). Также в сочетании с применяемыми методами и средствами можно означить атрибуты «Мастерство» или «Технический уровень». Общее количество итогового времени, необходимого на подготовку, можно учитывать для определения значения атрибута «Время».

Соответственно, учитывая затраченное время, можно постараться спрогнозировать деструктивное воздействие и итоговые последствия. На основе данных, полученных в ходе анализа оставленных следов, артефактов, а также периода до обнаружения APT, также можно определить атрибут «Незаметность». Инфор-

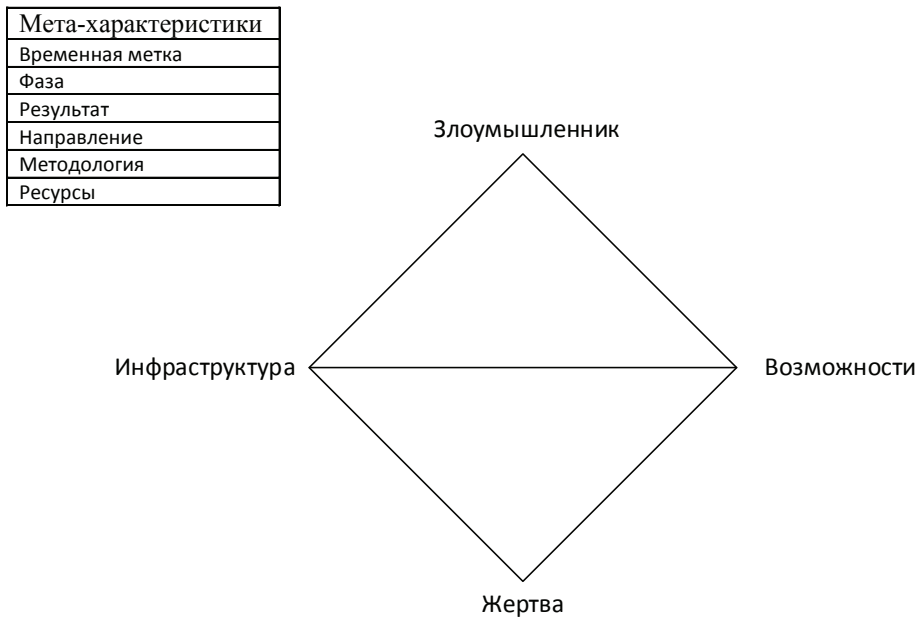

Рис. 4. Модель анализа вторжений Diamond [50]

мация об атакованном целевом объекте КИИ используется для определения атрибута «Специализация». В зависимости от принадлежности к той или иной категории КИИ, можно определить атрибут, характеризующий умение преодолевать защитные меры и проникать в целевую систему, например «Неудержимость». Итоговые последствия могут отражать уровень агрессии и другие атрибуты результатов выполнения APT. Сравнение различных цепочек реализации кибератаки дает возможность выявить сходство или отличие отдельных цепочек. По итогам анализа формируется профиль APT.

Следует отметить, что проанализированные модели обладают достаточным набором характеристик, необходимых для исследований целевых атак (APT). Они позволяют сформировать профиль нарушителя на абстрактном уровне. Исследуя цепочку этапов, эксперты и аналитики могут понять фазы APT, источники сбора данных, векторы атаки, определить применяемые методики реализации атаки и используемый инструментарий. Полученные сведения помогут сформировать профиль нарушителя, идентифицировать метрики для своевременного определения этапов цепочки кибератак и выявить возможность реализации атрибуции. Полученные в ходе анализа каждого жизненного цикла кибератаки данные в дальнейшем могут применяться для формирования набора профилей APT [37].

Рассмотренная модель активно применяется экспертами и исследователями [38]. Перспективным направлением является использование методов машинного обучения, в том числе глубокого обучения, для автоматизации процессов извлечения и идентификации соответствующих методов и средств, отдельных этапов цепочек, уникальных признаков APT и других функций, которые будут включены в процесс атрибуции [39-44]. В [45-49] предлагается решение задач обработки большого потока несортированных данных (сырых) и снижения количества ложных срабатываний (информационного шума).

3.3. Модель Diamond

Модель анализа вторжений Diamond Model (DM) описывает основные действия нарушителя в ходе кибератаки на основе определения возможных операций, выполняемых над инфраструктурой целевого объекта атаки. Данные действия называются в модели событиями.

В базовой версии [50] события включают четыре основных компонента: злоумышленник; возможности (злоумышленника); жертва (целевой объект, цель атаки); инфраструктура (целевого объекта). Компоненты соединены ребрами, которые подчеркивают взаимосвязь между ними (рис. 4).

- Злоумышленник — актор (нарушитель), атакующий жертву после анализа своих возможностей по реализуемым операциям над её инфраструктурой.
- Возможности - характеристики, описывающие инструменты и методы злоумышленника, применяемые в ходе кибератаки.

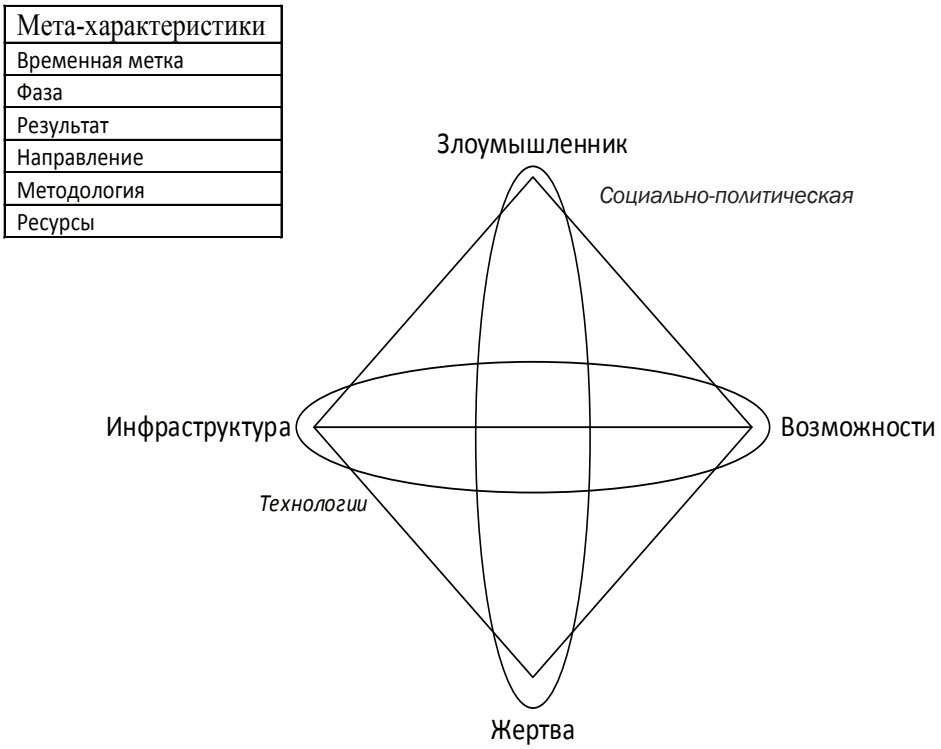

Рис. 5. Расширенная модель Diamond [51]

— Инфраструктура - описывает связи (физические и логические), которые злоумышленник использует для реализации возможностей по достижению результата.
— Жертва - цель, на которую осуществляется кибератака злоумышленника.

Для расширения свойств основных компонентов дополнительно присутствуют мета-характеристики (функции): временная метка (начало события, конец события), фаза, результат, направление, методология и ресурсы. Модель DM расширяется с помощью мета-характеристик. Описанные по умолчанию мета-характеристики не являются окончательными. Модель DM не ограничивается перечисленными выше компонентами.

3.4. Расширенная модель Diamond (Extended Diamond Model)

Расширенная модель Diamond (Extended Diamond Model, EDM) [51] дополнена двумя мета-характеристиками (признаками), отражающими (1) применяемые нарушителем технологии и (2) социально-политические мотивы. Технологии устанавливают взаимосвязь между инфраструктурой и возможностями, описывая методы и средства, позволяющие инфраструктуре и возможностям эффективно взаимодействовать. Например, если нарушитель применяет систему доменных имен (Domain Name System, DNS) для администрирования вредоносного решения в целях осуществления командования и контроля (C&C) над инфраструктурой жертвы, тогда DNS является частью технологий.

Взаимосвязь между злоумышленником и жертвой описывает социально – политическая (social-political) мета-характеристика. Она характеризует основные потребности, стремления и намерения нарушителя. Анализ таких данных позволяет выявить причину, по которой была выбрана жертва, её ценность для злоумышленника и как можно использовать данную взаимосвязь для противодействия нарушителю (рис. 5) [51].

Перемещаясь от одной вершины к другой, применяя полученные сведения в ходе анализа кибератаки, исследователи формируют гипотезы. Опровержение, доказательство или изменение данных гипотез в модели называется аналитическим вращением (Pivoting). Наличие установленных моделью компонентов позволяет сосредоточиться на конкретной вершине (функции) для целенаправленного («центрированного») анализа вторжения.

Таким образом, выполняя анализ со стороны жертвы, аналитики могут понять, как именно произошла кибератака, выявить уязвимые места и скомпрометированную инфраструктуру, со стороны инфраструктуры – возможности нарушителей, осуществляемые

действия в инфраструктуре (над инфраструктурой), и ориентируясь на нарушителя – сформировать область атакованных объектов, чтобы определить специализацию нарушителя.

В соответствии с данной моделью нарушитель выполняет последовательные действия, которые содержат минимум две результативные фазы для выполнения поставленной задачи. Такие действия называются потоком активности и имеют причинно-следственную связь. Потоки могут проходить по вертикали и горизонтали. Поток активности представлен в виде структурированного по фазам графа атак [52]. Вершина является событием, а дуги (ориентированные ребра) отражают причинно-следственные связи между событиями.

На рис. 6 изображен пример потока активности, отражающего действия нарушителей в отношении жертв. Связи, выделенные пунктиром, обозначают способность аналитиков объединять гипотезы. Такой подход позволяет заполнять пробелы в ходе анализа кибератаки. Подграфы этих потоков называются противоборствующими процессами, которые могут быть полезны позже для группировки и классификации действий на основе процесса, а не отдельных индикаторов.

Пример описания значений потока активности жертвы № 3, представлен в табл. 1.

Чтобы спрогнозировать потенциальный вектор атаки противника, в модели объединяются поток активности и граф атак в граф активности-атаки (рис. 7). Знания о действительных векторах атак интегрируются в множество гипотетических векторов для обозначения потенциальных или традиционных путей реализации атаки в будущем.

Для решения задач по атрибуции нарушителя, в модели предлагается концепция группы действий. Схожие сведения о кибератаке (инфраструктуре, возможностях, процессах и потоках) объединяются в группы общих (похожих) вредоносных событий. На основании таких данных формируются группы нарушителей. Группы могут включать в себя подгруппы и т.п. Концепция является гибкой и применима для идентификации любой группы нарушителей, в том числе APT.

Процесс формирования группы действий, включает шесть этапов:

1. Постановка аналитической задачи. Определяется аналитическая задача, которую необходимо решить с помощью группы действий;

2. Выбор метрик. Определяется набор метрик (показателей, характеристик), по которым измеряется сходство между кибератаками.

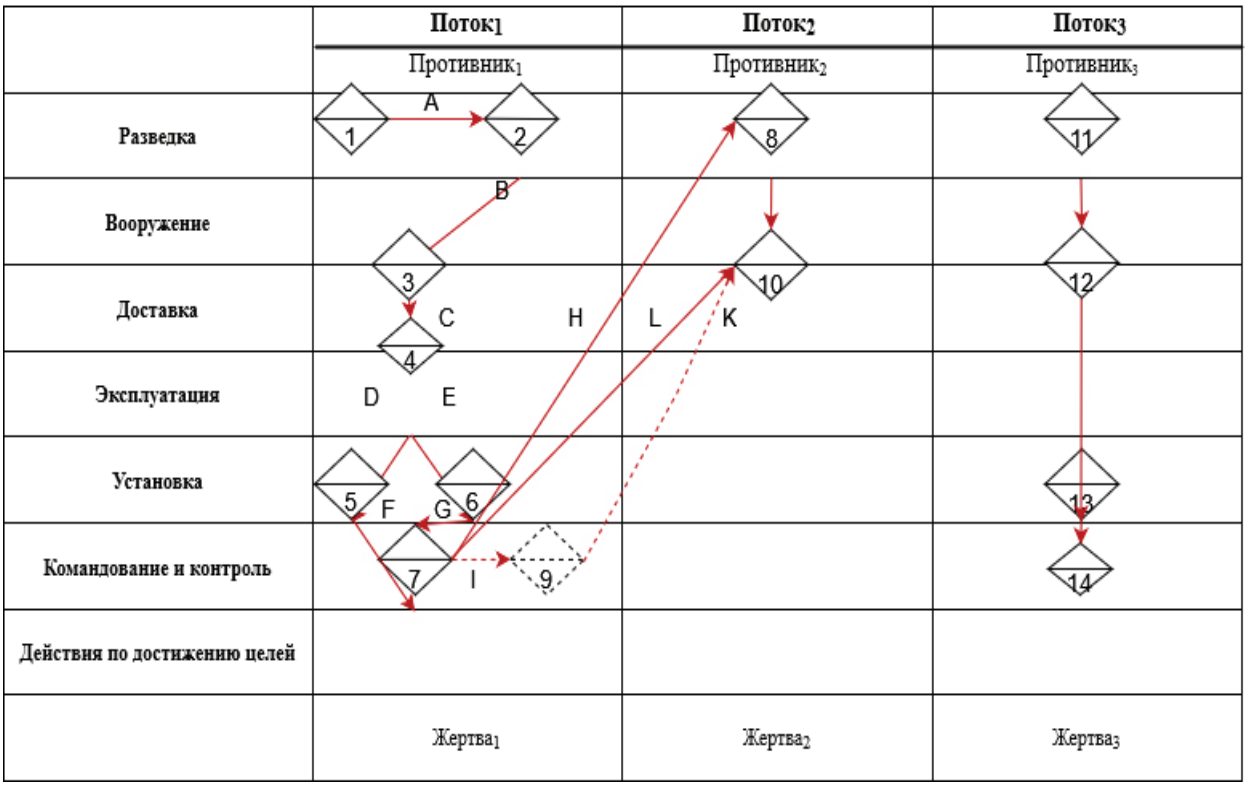

Рис. 6. Пример потока активности [52]

Таблица 1

Пример описания действий (потока активности) нарушителя

Фаза (этап)	№ события	Дуга	Действия нарушителя	Итог
Разведка (Reconnaissance)	11	M	Сканирование веб-сервисов на наличие уязвимостей	Результат сканирования сообщает о наличии уязвимых веб-сервисов и возможности применения эксплойта
Вооружение (Weaponization)			Подбор эксплойта	Эксплойт найден
Доставка (Delivery)	12	N	Доставка эксплойта жертве по сети	Доставка осуществлена успешно
Эксплуатация (Exploitation)			Запуск эксплойта	Запуск осуществлен успешно
Установка (Installation)			Установка на уязвимый сервер жертвы средств удаленного администрирования	Установка завершена успешно
Командование и контроль (Command & Control)	13	O	Соединение с компрометированным сервером	Получен доступ к средствам удалённого администрирования, сервер доступен для выполнения удаленных команд
Выполнение действий (Action on Objectives)	14		Выгрузка конфиденциальных данных	Данные успешно загружены нарушителем

3. Создание группы. Путем кластеризации похожих сведений по заданным метрикам формируется группа действий.

4. Рост группы. Расширение группы действий за счет обогащения дополнительными сведениями.

5. Анализ. Группа действий анализируется на предмет решения и дополнения аналитической задачи.

6. Переопределение. Для поддержания групп действия в актуальном состоянии, производится их пересмотр на основе обновленных сведений.

Одним из преимуществ данной модели является предоставление списка функций, которые должны присутствовать в каждом событии. Данный подход повышает эффективность модели, так как позволяет выявлять пробелы в знаниях о кибератаке и с помощью множества гипотез устранять недостатки в аналитических сведениях [53]. Модель устанавливает основу для онтологий, таксономий, протоколов обмена информацией о киберугрозах и управления знаниями. Модель может дополняться на определенных уровнях другими моделями. Например, интеграция с моделью UKC позволит улучшить результаты при анализе отдельных этапов действий нарушителя [54]. Модель может также использоваться для анализа вторжений и классификации событий в реальном времени на основе применения аналитического подхода и структурирования данных об уже исследованных нарушителях (кибератаках). Можно отметить, что модель обладает широким потенциалом для применения для атрибуции нарушителей [55].

3.5. Модель (матрица) MITRE ATT&CK

Модель ATT&CK (Adversarial Tactics, Techniques & Common Knowledge - тактики, техники и общие знания о кибератаках), еще называемая матрицей или базой знаний, основана на реальных событиях и содержит информацию о методах, методиках и процедурах, применяемых нарушителями. Информация в базе знаний MITRE ATT&CK представлена в виде набора матриц.

Представим ниже основные компоненты модели MITRE ATT&CK [56]: тактики; техники; подтехники; процедуры.

Тактики обозначают промежуточные или основные цели нарушителя во время реализации кибератаки. Каждая тактическая категория включает в себя техники и подтехники (субтехники).

Техники составляют приёмы, помогающие нарушителям для достижения основных целей.

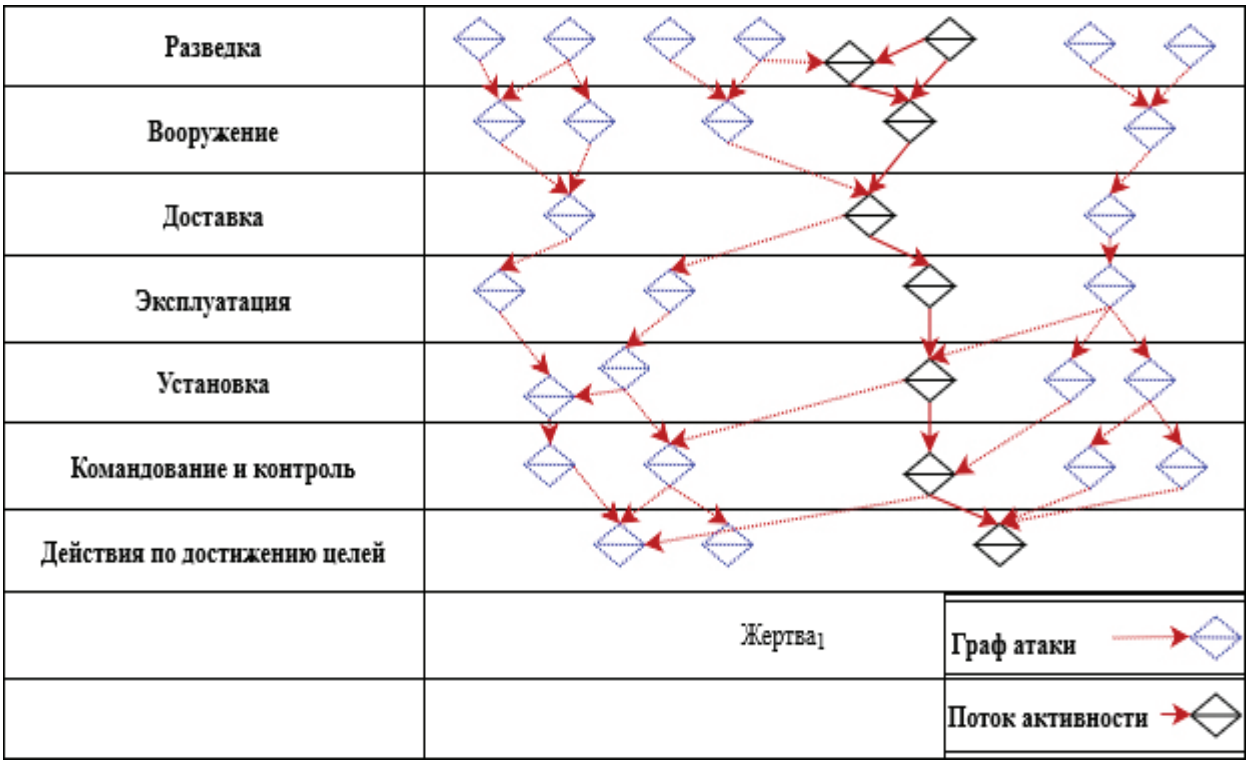

Рис. 7. Пример графа активности – атаки [52]

Подтехники (инструментарий) представляют собой более детальное описание на низком уровне техник, включающее сведения об инструментарии.

Процедуры реализуют конкретные случаи применения техник и подтехник.

Формальную взаимосвязь между отдельными компонентами модели можно отобразить в виде диаграммы (рис. 8).

Модель представлена в виде технологических доменов и включает следующие области применения: (1) MITRE ATT&CK Enterprise - корпоративный сегмент; (2) MITRE ATT&CK Mobile - для мобильных устройств; (3) MITRE ATT&CK Industrial Control Systems (ICS) - промышленные системы управления, такие как автоматизированные системы управления технологическим производством (АСУ ТП) и системы диспетчеризации и сбора данных (SCADA).

В корпоративном сегменте на данный момент выделено четырнадцать тактик [57]:

- разведка - нарушителями ведется сбор полезной информации для планирования и совершенствования кибератаки;
- развитие ресурсов - этап предполагает подготовку инфраструктуры, необходимой для вторжения, и расширения возможностей инструментария;
- первоначальный доступ - нарушителями осуществляется попытка осуществления доступа к информационным ресурсам целевого объекта; делается попытка закрепиться в сети жертвы;
- реализация - запуск вредоносного кода (реализация инструментария) на подконтрольном узле или системе; на данной стадии, атакующие пытаются расширить свои возможности в инфраструктуре жертвы;
- обеспечение постоянного присутствия - обеспечение длительного доступа к скомпрометированной среде на основе применения методов, позволяющих осуществлять устойчивый доступ в условиях изменения скомпрометированной среды;
- повышение привилегий - нарушители осуществляют попытки расширить свои права, получить более высокие привилегии в целевой системе;
- уклонение от защиты - нарушителями применяются методы обхода средств защиты и сокрытия своего присутствия в целевой системе;
- доступ к учетным данным - манипуляция учетными данными пользователей, информационных систем, служб с целью получения санкционированного доступа к скомпрометированной инфраструктуре жертвы;

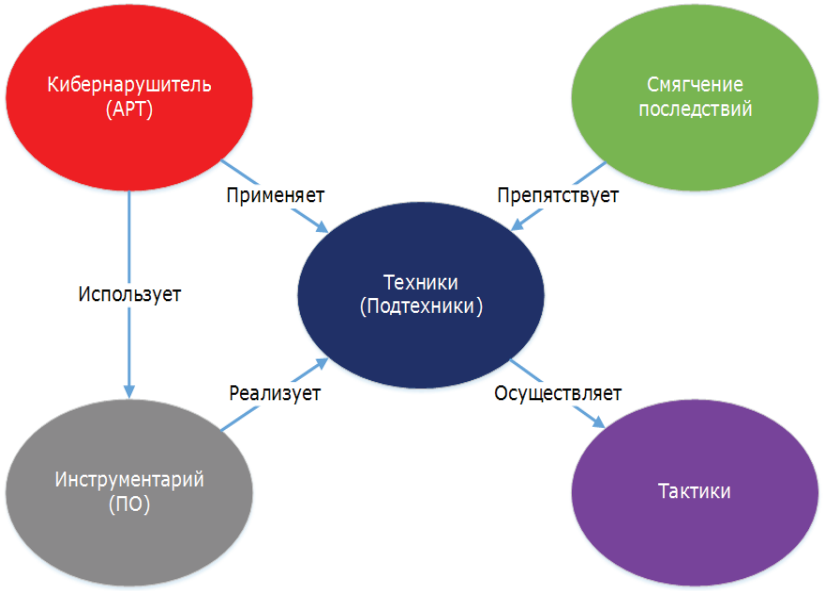

Рис. 8. Взаимосвязи модели MITRE ATT&CK [56]

— обнаружение — нарушители производят сбор сведений об инфраструктуре с целью реализации кибератаки;
— боковое смещение — перемещение внутри скомпрометированной инфраструктуры за счет информационных ресурсов жертвы для достижения основной цели;
— сбор данных — нарушителями применяются методы идентификации и агрегации конфиденциальных данных в скомпрометированной среде для их кражи, изменения или уничтожения;
— командование и контроль — нарушителями применяются методики для обеспечения связи и администрирования управляемой ими инфраструктуры;
— эксфильтрация — выгрузка (хищение) данных из целевой среды;
— причинение ущерба — воздействие на инфраструктуру жертвы для реализации цели атаки и сокрытие следов или затруднение противодействия.

Для категоризации и описания действий нарушителей на ранних стадиях жизненного цикла реализации кибератаки, тактики «Разведка и Развитие ресурсов» классифицированы в качестве подготовительного этапа (PRE Matrix). Выделяется десять базовых техник на этапе разведки и семь техник на этапе подготовки ресурсов. В качестве дополнительной детализации и повышения сравнительных характеристик действий нарушителей на начальном этапе PRE Matrix можно интегрировать в модель СКС. В отличие от модели СКС, в модели ATT&CK тактики не образуют последовательность, а предполагаются выборочные действия нарушителей.

Модель ATT&CK включает в себя классификацию известных группировок или отдельных акторов, отслеживаемых государственными и частными организациями в сфере киберприступлений. Сведения о них сгруппированы в отдельный профиль и включают следующие характеристики [58]:

— название группировки;
— уникальный идентификатор (id);
— связанные группировки (кибератаки);
— описание;
— применяемые техники и подтехники;
— инструментарий.

Говоря о КИИ, отдельно стоит выделить подмодель MITRE ATT&CK для систем промышленного управления (MITRE ATT&CK Industrial Control Systems) [59, 60]. Именно индустриальные системы отвечают за технологические процессы КИИ. Основной фокус сделан на методах нарушителей, цель которых состоит в причинении ущерба промышленным системам (процессам). Отличия от модели для корпоративного сегмента являются несущественными. Всего выделено двенадцать тактик:

— первоначальный доступ;
— реализация;
— обеспечение постоянного присутствия;
— повышение привилегий;
— уклонение;
— обнаружение;

— боковое смещение;
— сбор данных;
— командование и контроль;
— подавление функции отклика (функция запрета реагирования) - действия нарушителей направлены на блокировку функций оповещения оператора системы об инцидентах безопасности, установленных для технологических процессов; происходит маскировка деструктивного воздействия на систему путем предотвращения ожидаемых сигналов тревоги на сбои, критические отклонения от заданных сценариев в работе; в отличие от методов применяемых на стадии «уклонение», приемы подавления функции отклика могут быть более интрузивными, например, активная блокировка реакции на базовые события безопасности;
— нарушение управления процессами - манипуляция, нарушение или отключение контролируемых физических процессов в целевой среде; часто применяется с тактикой «Подавления функции отклика»;
— причинение ущерба.

Матрица промышленных систем предлагает базовые определения поведения нарушителей в данной среде. В своей области проект является авторитетным и перспективным для применения в системе атрибуции нарушителей при целевых атаках на объекты КИИ. В целях детального анализа и повышения качества атрибуции, можно рассмотреть (исследовать) применение матрицы в сочетании с выше рассмотренными ее компонентами и моделями анализа вторжений.

За исключением традиционного назначения (моделирование угроз, смягчение последствий, планирование киберучений) модель MITRE ATT&CK может использоваться в качестве поведенческой модели нарушителей (APT) и описывать действия на протяжении всего жизненного цикла кибератаки [61]. На основе имеющихся профилей кибергруппировок модель MITRE ATT&CK позволяет проводить атрибуцию методом классификации полученных данных по характерным для конкретных APT признакам (сигнатурам). Кроме того, эта модель может выступать источником обогащения существующей базы профилирования APT [62].

4. Методики и системы для атрибуции кибернарушителей

Проведем обобщенный анализ подходов к реализации методик и созданию автоматизированных систем атрибуции и представим несколько примеров разработанных методик и реализованных систем, которые можно использовать для атрибуции кибернарушителей.

4.3. Обобщенный анализ подходов к реализации методик и созданию автоматизированных систем атрибуции

КИИ подвергаются многомерным киберугрозам, в которых сложно выделить границы между информационными технологиями и промышленными системами - перемещаясь по сетям, атакующие используют информационные технологии для выбора и реализации вектора атак на АСУ ТП [63]. Следовательно, необходимо применять комплексный (гибридный) подход для анализа и атрибуции целевых атак на КИИ [64, 65].

Важнейшим элементом при выполнении атрибуции является сбор необходимых данных. Данные, которые собираются, обрабатываются и анализируются для понимания мотивов, целей и поведения нарушителя [66, 67]. Применяемые стандарты, например, XML, JSON, CybOX/STIX, OpenIOC, IODEF, CAPEC и MAEC позволяют детально описывать инциденты кибербезопасности [68]. Общепринятыми протоколами обмена данных об угрозах являются TAXII и STIX [69]. Их использование делает обмен данными своевременным и безопасным. Предлагаемый подход CyberSANE [70] направлен на работу с моделями анализа вторжений, способными определять скрытые и косвенные векторы кибератак на целевую систему, в том числе атаки, которые используются APT, программы-вымогатели и ботнеты. Аналитика угроз основана на сборе данных из открытых источников, социальных сетей, специализированных форумах, даркнете и т.п.

Данные о нарушителях разделяются на три типа:
— тактические – информация технического характера, получаемая от различных индикаторов компрометации;
— операционные – сведения для формирования профиля, например, о тактиках, техниках и процедурах (ТТП). Специализации, возможностях, географической локации и т.п.;
— стратегические – данные о возможном ущербе в случае деструктивного воздействия на целевой объект.

Чтобы обеспечить структурированный формат данных, процесс обработки информации проходит несколько стадий (рис. 12):
— планирование процедур сбора и обработки необходимых данных и процедур их анализа для

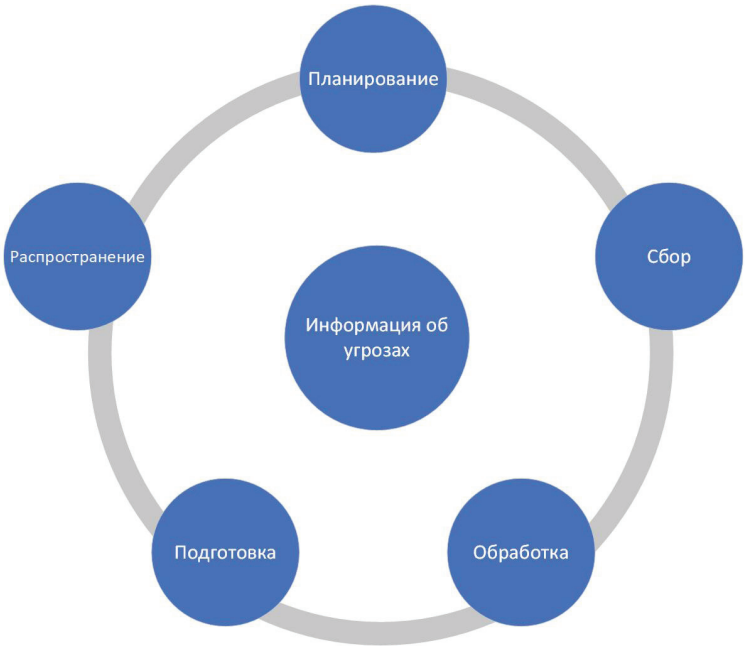

Рис. 12. Цикл формирования данных о киберугрозах [67]

автоматизированного или ручного выполнения сценариев;

— сбор и обработка данных – сбор необходимой информации, организация единого формата, удаление дубликатов данных. Обработка включает оперативный поиск и извлечения конкретных сведений, кластеризация данных;
— подготовка – анализ данных, выявление недостатков в работе алгоритмов, применяемых на ранних этапах. Исследование на предмет подозрительного или вредоносного содержания;
— распространение – передача данных о киберугрозах, в том числе компоненту атрибуции, обеспечивая обогащение информацией по анализу угроз [67].

Использование аналитики угроз входит в состав большинства современных решений по обнаружению и атрибуции APT [71, 72]: Kaspersky Threat Intelligence Portal, IBM X-Force Exchange, Anomali ThreatStream, SolarWinds Security Event Manager, Palo Alto Networks Cortex XSOAR TIM и др.

Данный подход поддерживает возможность автоматизации, обновления в режиме реального времени, интеграции с различными системами, применения методов искусственного интеллекта и машинного обучения.

Наличие стандартов описания угроз и протоколов обмена данными, позволяют автоматизировать процесс атрибуции. Ввиду нехватки подготовленных специалистов, автоматизация является приоритетным направлением у большинства организаций. Применение методов машинного обучения позволяет повысить эффективность операций атрибуции [73].

Широкое применение обновлений в режиме реального времени дает возможность своевременно обогащать структурированными данными базу профилей нарушителей (APT), поддерживая ее в актуальном состоянии [72].

Для повышения эффективности процессов анализа целевых кибератак и атрибуции важна интеграция систем атрибуции с SIEM-системами и другими системами управления безопасностью, позволяя анализировать и коррелировать информацию из других источников.

Улучшать атрибуцию можно за счет интеграции перспективных методик. В [74] аналитика киберугроз, основанная на правилах ассоциативного анализа данных, позволяет идентифицировать кибератаку, связывать ее с нарушителем, а также удалять избыточные сведения, не связанные с атрибуцией кибератаки.

Возможность применения искусственного интеллекта и машинного обучения, повышает процессы автоматизации и интеллектуализации, в целом позволяя добиться более качественных результатов при атрибуции нарушителей, осуществляющих целевые атаки на КИИ [75].

Перспективные алгоритмы машинного обучения в сфере кибербезопасности, а также возможные векторы атак на интеллектуальные системы, применяющие такие алгоритмы рассмотрены в [76]. Таксономия алгоритмов машинного обучения, хорошо зарекомен-

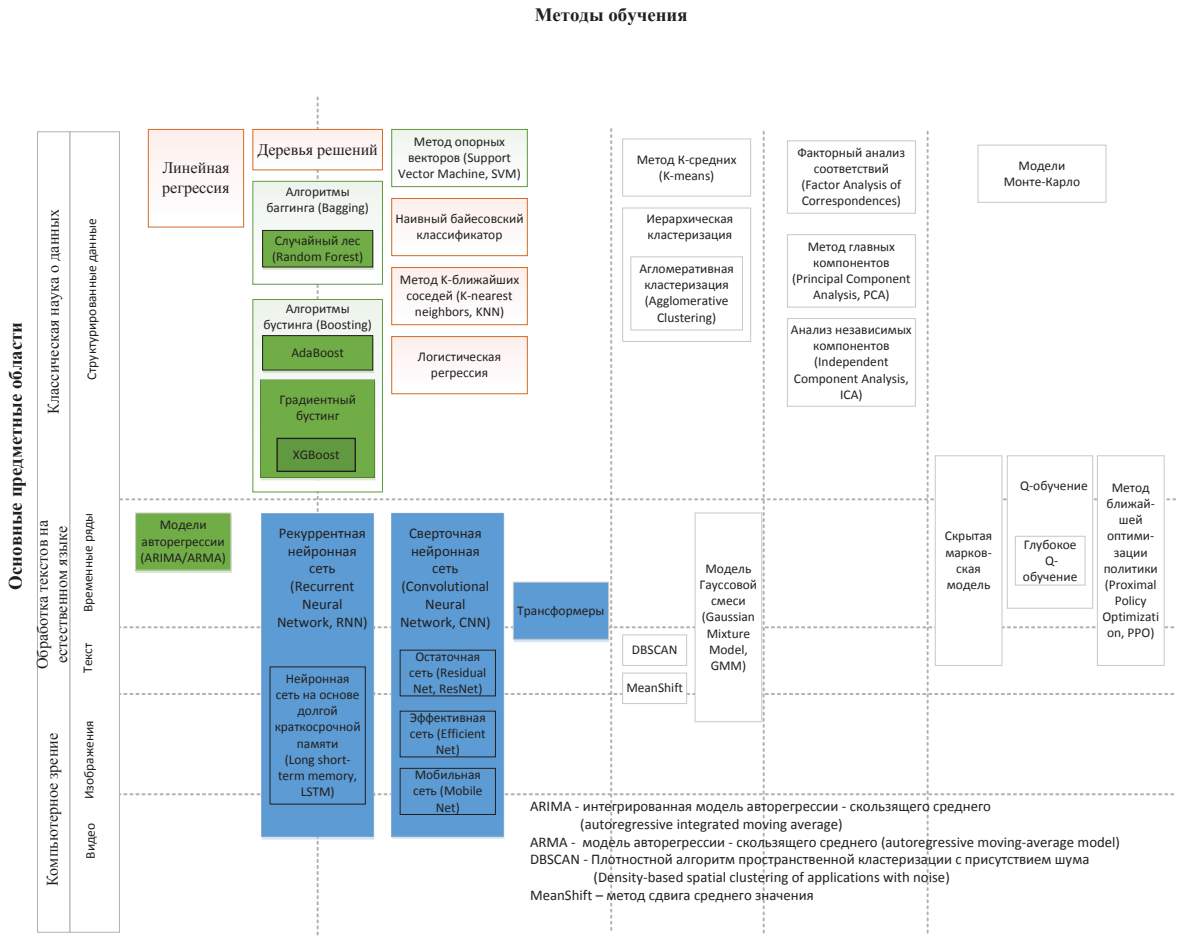

Рис. 9. Таксономия алгоритмов машинного обучения [76]

довавших себя при решении этих задач, представлена на рис. 9 (необходимые пояснения и соответствия на английском даны на рисунке).

В большом количестве работ, например [77-81], выполнен анализ применения методов глубокого обучения для обнаружения кибератак, в том числе на КИИ, и решения задач атрибуции кибернарушителей.

Обнаружение APT с использованием методов машинного обучения в некоторых случаях дает высокие результаты. Например, применение вариантов искусственной иммунной системы и рекуррентных нейронных сетей для обнаружения APT, показало, что предложенные алгоритмы обеспечивают не только возможность обнаружения, но и позволяют провести атрибуцию APT с точностью от 62 до 99,20% [82].

В работе [83] удалось с высокой точностью выявить APT в реальном времени и провести классификацию кибератак. В работе [84] автоматизированное профилирование APT с применением машинного обучения на основе шаблонов целевых атак позволило обеспечить значения точности атрибуции от 83 до 94%. Метод аргументированного рассуждения с доказательствами на техническом и социальных уровнях для атрибуции кибератак представлен в работе [85]. Методика использования технических артефактов для выявления ложных флагов при атрибуции целевых кибератак представлена в [86]. Рассмотрим ниже две последние методики более детально.

4.2. Методика и система атрибуции, основанные на аргументированном рассуждении (argumentation-based reasoner, ABR)

В [85] предложены методика и исследовательский прототип системы атрибуции на основе аргументации, которые призваны помочь исследователям и специалистам в процессе атрибуции кибератак.

Архитектура ABR состоит из двух основных компонентов: компонента вывода (рассуждений) и базы знаний (рис. 10).

ABR использует как технические, так и социальные доказательства (свидетельства), полученные в ходе анализа целевой кибератаки. При обработке входных данных нетехнического характера используется социальная модель атрибуции, называемая Q-моделью [87]. Доказательства и правила аргументированного рассуждения разделяются на три уровня: технический, операционный и стратегический. Комбинация информации на этих уровнях направлена на имитацию процесса расследования киберинцидентов в целях атрибуции кибератак.

Технический уровень состоит из правил, которые касаются доказательств, полученных в результате процесса расследования инцидентов, связанных с техническими аспектами реализации атаки и тем, как она была осуществлена (трафик, логи и др.). На этом уровне определяются, например, IP-адрес, с которого была совершена атака, время атаки, данные журналов (системы логирования), тип атаки, используемый код.

Операционный уровень состоит из правил, касающихся нетехнических доказательств, относящихся к социальным аспектам. На этом уровне выявляются, например, сведения о том, где произошла кибератака, ее возможные мотивы, необходимые возможности для ее совершения, политический или экономический контекст данной целевой атаки.

Стратегический уровень состоит из правил, относящихся к идентификации кибернарушителя. На этом уровне определяются, например, сведения о том, кто совершил атаку, кому она была выгодна.

Правила операционного уровня используют информацию, полученную от технического уровня, а правила стратегического уровня используют информацию, полученную от технического и операционного уровней. Все три уровня используют данные, предоставленные пользователем, а также фоновые знания. Эта категоризация доказательств и правил на трех уровнях направлена на то, чтобы подражать анализу следователя в процессе расследования кибератаки и атрибуции кибернарушителя, когда следователь переходит от технического уровня к операционному и от операционного к стратегическому, используя выводы из предыдущих уровней. Кроме того, данная категоризация повышает удобство использования ABR, учитывая знания следователя на всех уровнях.

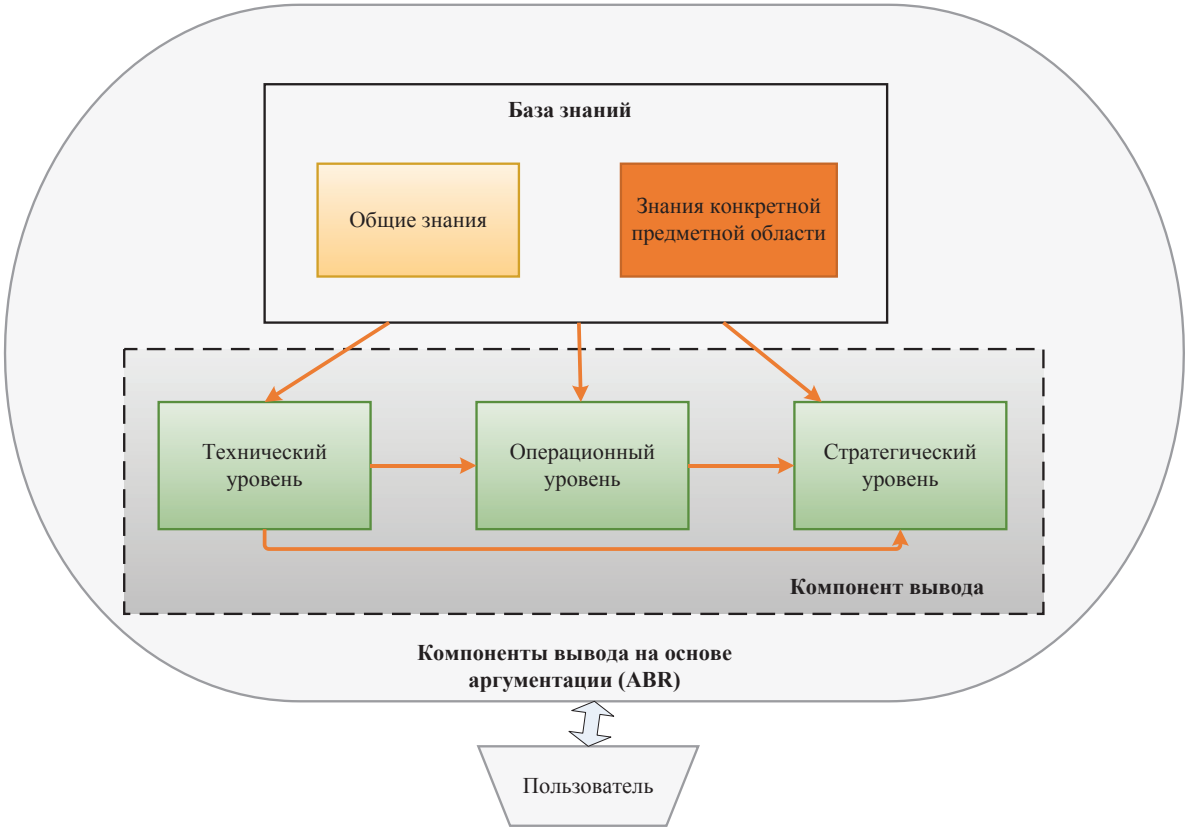

Рис. 10. Компоненты аргументированного рассуждения [85]

Основываясь на реальных кибератаках из общедоступных источников, ABR включает в себя около двухсот правил рассуждений. Данные правила были преобразованы в общие правила аргументации и являются одним из основных компонентов ABR. Взаимодействуя между собой на разных уровнях, правила позволяют выполнять рассуждения, лежащие в основе атрибуции реальных кибератак. Они также подразделяются на три уровня: технический, операционный и стратегический.

Знания подразделяются на общие знания и знания, относящиеся к предметной области. Кроме знаний и данных о реальных атаках, в своей работе ABR также использует фоновые знания, содержащие информацию, не относящуюся к конкретным случаям (целевым кибератакам). Применение фоновых знаний помогает минимизировать ошибки, связанные с человеческим фактором. Набор данных состоит из фрагментов информации, которые используются правилами вывода в качестве предварительных условий для ответа на запросы пользователя (исследователя, аналитика). Фоновые знания ABR могут быть обновлены и обогащены пользователем. Стоит отметить, что получение осмысленных выводов посредством применения правил к знаниям зависит от правильности предоставленных знаний.

Общие знания состоят из информации о характеристиках стран, международных отношениях между ними и классификации организаций и промышленных предприятий и др. Эта информация используется вместе с предоставленными доказательствами (свидетельствами) для проведения анализа. К данной категории также относятся данные о киберпотенциале и возможностях государств. Оценивая киберпотенциал государства, можно ограничивать типы атак, которые могут входить в состав реализуемых целевых атак. В качестве источников этой информации могут служить, например, данные группы глобального индекса кибербезопасности (Global Cybersecurity Index, GCI) [88] и кибервозможности стран, участвующих в кибервойне [89]. GCI представляет собой составной индекс, объединяющий 25 показателей в один эталонный показатель для мониторинга и сравнения уровня обязательств государств в отношении кибербезопасности. Выделяется три группы стран: ведущие, развивающиеся и инициирующие. Кроме того, на основе кибервозможностей в кибервойне [89] некоторые страны определяются, как киберсверхдержавы (США, КНР, Российская Федерация, Израиль, Великобритания).

Знания предметной области состоят из информации об известных APT, отдельных кибергруппировках и осуществленных кибератаках. Данная информация в основном используется на стратегическом и техническом уровнях. Известные APT включают следующий набор атрибутов: название или идентификатор; страна происхождения; страны/организации, на которые кибергруппировка обращала внимание в прошлом; вредоносное ПО или фрагменты вредоносного ПО (подозреваемые или подтвержденные), связанные с кибергруппировкой, а также отношения этой кибергруппировки с другими субъектами (например, правительствами). Еще одна важная часть предметно-ориентированных знаний — сходство с прошлыми целевыми атаками. Например, сходство с вредоносной программой, связанной с конкретной APT, может указывать на то, что за кибератаку может нести ответственность одна и та же кибергруппировка.

Полученные в ходе работы ABR результаты являются аргументами для новых гипотез исследования кибератаки. Использование аргументированного подхода, основанного на предпочтениях и абдуктивных рассуждениях [90], позволяет ABR работать с противоречивыми доказательствами (гипотезами) и заполнять пробелы в знаниях, возникающие из-за неполноты данных.

Представленная в [83] методика позволяет осуществлять атрибуцию кибернарушителей итеративно, делая выводы прозрачно для аналитиков. Несмотря на способность осуществлять атрибуцию и выстраивать гипотезы, ABR сильно зависит от правильности предоставленных данных. Основная цель ABR - помочь аналитику в процессе анализа и предоставить полезную информацию. Говоря о перспективной системе атрибуции в целом, применение методики рассуждения на основе аргументации может рассматриваться как дополнительное средство автоматизации, повышая быстродействие и точность процесса атрибуции кибернарушителя.

4.3. Методика использования технических артефактов для выявления ложных флагов при атрибуции целевых кибератак

Ложный флаг [91] относится к тактике, применяемой кибернарушителями с целью скрыть деструктивную активность в ходе целевой кибератаки или скрыть свое присутствие, обвинив в реализации кибератаки третью сторону. В [86] предлагается модель атрибуции кибернарушителя с применением технических артефактов (цифрового следа). Каждое деструктивное воздействие способно оставлять после себя артефакты [86].

Предполагается, что анализируя цифровой след кибернарушителя, аналитики формируют входные данные для процесса атрибуции кибератаки. Не сумев выявить сфальсифицированные сведения, процесс атрибуции пойдет по ложному сценарию. В отличие от простого обнаружения атак, атрибуция фокусируется на связи действий с действующими лицами. Поэтому важной задачей становится определение профилей акторов [92], которые используются для сравнения действий с известными профилями, зафиксированными в уже реализованных APT. Зная, какие следы оставляют злоумышленники, можно определить, какие из них достаточно уникальны, а какие можно легко подделать, запутав расследование.

В соответствии с базовой моделью «цепочка кибервторжений» [23], в [86] все следы (артефакты) кибернарушителей условно подразделяются на артефакты разведки, вооружения, доставки, эксплуатации, установки, управления и контроля, а также действий.

К артефактам разведки относятся активные попытки сканирования на сетевом уровне, действия по анализу профилей на сайтах социальных сетей, фишинг для сбора информации, атаки методом перебора паролей на внешние сервисы, например веб-почту и т.п.

Артефакты вооружения представляются данными о первоначальной технике проникновения, в том числе насколько сложной она была и сколько усилий потребовалось кибернарушителю, использовались ли известные уязвимости и известный инструментарий или были задействованы совершенно новые, разработанные специально для исследуемой кибератаки. Анализ следов вооружения позволяет собрать атрибуты о возможностях и ресурсах злоумышленников.

К артефактам доставки относятся пути доставки вредоносного ПО (электронная почта, мгновенные сообщения, интернет-форум, SQL-инъекция, попутная загрузка и т.д.) и связанная с ними информация (идентификаторы, URL-адреса и т.п.).

Артефакты эксплуатации определяются атрибутами, метаданными, дизайном и функционалом вредоносного ПО. Индикаторами целенаправленной атаки являются использование редкой уязвимости или эксплойта, адаптированного к целевой среде.

Фаза установки обычно включает в себя довольно сложные действия, которые выполняются индивидуально в зависимости от злоумышленника и от жертвы. В группу артефактов установки включают следы, характеризующие используемые при установке методы и процедуры, данные файлов журналов, мониторинга сети и затронутых хостов, а также результаты криминалистической экспертизы использованных вредоносных программ (например, остатков файлов) и рабочих станций.

Вопросы аналитиков, касающиеся фазы управления и контроля, сосредоточены на фактической инфраструктуре, используемой кибернарушителями. Эффективная инфраструктура для командования и контроля требует больших затрат на установку и обслуживание, ее часто повторно используют или сдают в аренду. Артефакты управления и контроля, которые могут помочь в процессе атрибуции: журналы DNS, информация о домене, применяемые методы уклонения от обнаружения.

На этапе выполнения действий кибернарушители часто раскрывают информацию о себе, например, используя известную зону сброса для извлеченных данных или выполняя действия, связанные с событиями в физическом мире (например, нанося ущерб посредством кибератаки в ответ на политические события). К артефактам действий относят: аномальный сетевой трафик, данные журналов с эксплуатируемых рабочих станций, используемые инструменты и их конфигурацию, применяемую внешнюю инфраструктуру.

В [86] утверждается, что атрибуция кибернарушителей заключается в том, чтобы задавать правильные вопросы и давать правдоподобные ответы (строить гипотезы). Данный процесс сравнивается с игрой в головоломку - разные части обнаруживаются в любой последовательности, но в конечном итоге они должны складываться в единую картину. Предлагаемая модель атрибуции кибернарушителей (Cyber Attribution Model, CAM) [86] состоит из двух основных компонентов (рис. 11): (1) расследования кибератак и (2) профилирования субъектов киберугроз.

Атрибуция происходит путем сопоставления этих компонентов. Каждый компонент использует технические и социально-политические индикаторы в сочетании с компонентами CAM-подхода. Основная цель расследования кибератаки - ответить на вопросы, кто жертва и почему, а также что произошло и как.

Ответы на эти вопросы определяются компонентами (1) виктимология, (2) инфраструктура, (3) возможности и (4) мотивация.

Они помогают обнаруживать способы и методы реализации конкретной кибератаки, необходимые возможности кибернарушителей, а также возможные «ложные флаги». Целью профилирования субъектов киберугроз является разработка профилей на основе прошлых атак и поиск профиля, соответствующего выводам на основе расследования кибератак.

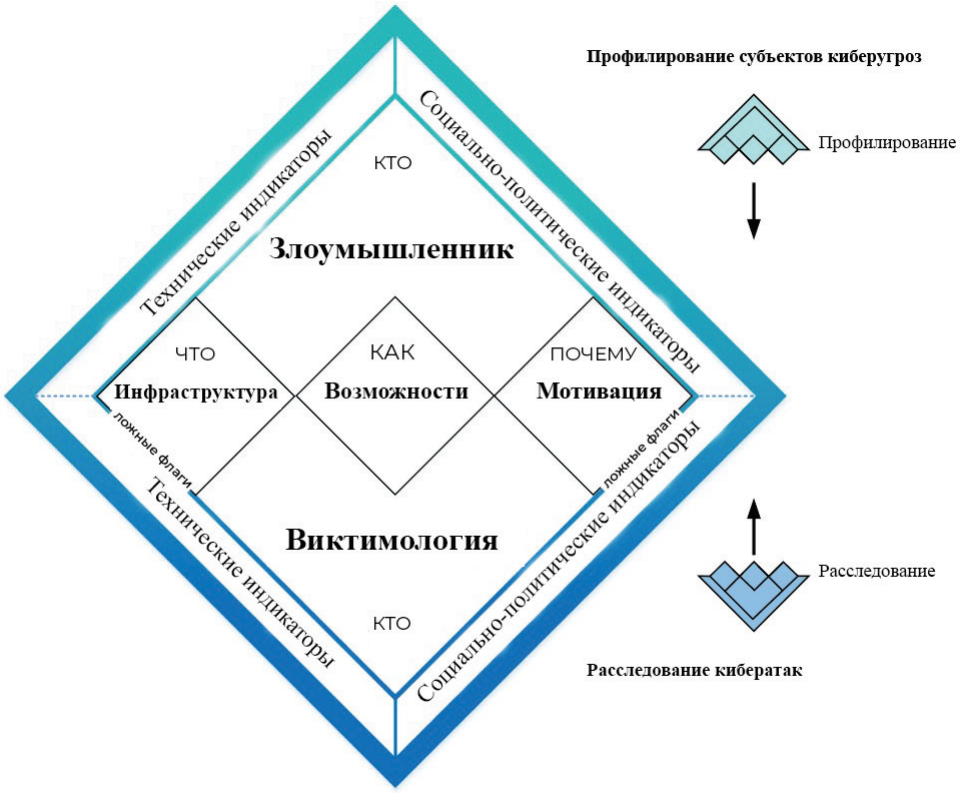

Рис. 11. Модель кибератрибуции (CAM), применяемая для выявления несоответствий (ложных флагов) в процессе атрибуции [92]

Профилирование субъектов киберугроз осуществляется либо непрерывно, либо по мере необходимости для поддержки расследований. В последнем случае компонент (1) и компонент (2) выполняются параллельно, чтобы найти соответствие между примененными методами и возможными профилями кибернарушителей. В обоих компонентах технические и социально-политические индикаторы помогают понять факты и распознать сложные взаимосвязи и возможные операции под ложным флагом. Профилирование субъектов киберугроз аналогично профилированию в других областях. Поскольку технологии быстро меняются, аналитики должны постоянно быть в курсе новейших методов реализации атак. Таким образом, профилирование субъектов киберугроз направлено на периодическое создание, обновление и управление профилями субъектов угроз (кибернарушителей).

С технической точки зрения процесс атрибуции (рис. 11) заключается в обнаружении источника базовых данных, сборе аналитиками артефактов, извлечения полезных данных и формировании ответа на ключевые вопросы:

Вопрос 1. Сколько усилий (например, требуется большая команда, большое количество рабочих часов) требуется кибернарушителю для подделки артефакта, либо изменения своих действия для создания других следов?

Вопрос 2. Сколько специальных знаний требуется, чтобы манипулировать соответствующими артефактами и оставлять лишь незначительные следы?

Вопрос 3. Насколько сложно обнаружить следы манипуляций или маскировки?

Вопрос 4. Насколько уникальны и/или детализированы потенциальные следы (артефакты)?

Вопрос 5. Насколько тесно связаны другие артефакты (важно для создания целостной картины)?

Для выполнения атрибуции на первом этапе аналитики определяют, какие источники данных доступны. В качестве источников данных может выступать рассмотренная матрица MITRE ATT&CK [56]. Кроме того, необходимо учитывать дополнительные (в основном внешние) источники данных, включая каналы информации об угрозах, социальные сети и новостные ленты. Как только потенциально релевантные источники будут определены, исследователи собирают артефакты, получают информацию более высокого уровня и формулируют ключевые вопросы в ходе процесса атрибуции.

Рис. 11. Упрощенное представление процесса атрибуции

Основанная на тщательной оценке технических следов, атрибуция направлена на то, чтобы лучше понять точку зрения злоумышленника. В этом процессе анализ артефактов, рассмотренных ранее, позволяет дать ответы на вопросы, касающиеся инфраструктуры жертвы (и любой третьей стороны), возможностей актора и его конкретной мотивации. Многие отдельные свойства кибератаки могут быть сфальсифицированы и замаскированы, например, IP-адрес скрывается с использованием (цепочек) прокси-серверов или сети TOR, злоумышленники выдают себя за других, фальсифицируют языковые настройки, вводят ложные артефакты в коде и т.п. Тем не менее, довольно сложно правильно собрать все эти цифровые следы. Тщательная атрибуция должна уделять особое внимание всей последовательности действий. Если какой-то один фактор выглядит странно или не вписывается в очевидный сценарий, его необходимо перепроверить, совершив повторный анализ.

Следует отметить, что «ложные флаги» всегда присутствуют по следующим причинам:

- применяемые кибернарушителями эксплойты содержат переработанный код или использовались раннее и стали общедоступны;
- разрабатывается специализированное ПО для имитации поведения и увеличения сложности атрибуции вредоносных программ;
- чаще всего эксплойты и вредоносные программы покупаются, а не разрабатываются;
- инструментарий для целевых кибератак можно взять в аренду как услугу;
- на этапе «командование и контроль», вредоносное ПО использует известную инфраструктуру (третьих лиц), которая не относится к операторам вредоносного ПО;
- применяются методы социальной инженерии с целью направить расследование по ложному сценарию;
- выполнение действий с целью скрыть следы или в вести аналитиков в заблуждение (например, с использованием шифрования данных).

В перспективной системе атрибуции кибернарушителей при реализации ими целевых атак на объекты КИИ должен присутствовать компонент распознавания (поиска) «ложных флагов».

Заключение

В данной работе представлен анализ актуальных моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых кибератак на объекты критической инфраструктуры. Рассматриваемый класс угроз – целевые атаки на объекты КИИ, важным подклассом которых являются продвинутые постоянные угрозы (APT), - требует многоуровневой классификации на каждом этапе жизненного цикла кибератаки.

Применение моделей «цепочка кибервторжений» CK и UKC для описания этапов вторжения, сопоставления индикаторов на различных фазах действия APT, выявление закономерностей, связывающих отдельные вторжения с более широкими кампаниями по реализации кибератак, позволяет формировать данные для понимания итеративного характера целевых атак и реализации предварительной атрибуции нарушителя и целевых кибератак.

Модели анализа вторжений DM и EDM позволяют проводить высокоуровневую атрибуцию с учетом не только анализа методик, методов и инструментария реализации кибератак, но и социально-политического контекста, выстраивая причинно-следственные связи, а также поддерживать атрибуцию и выявление целевых кибератак.

Дополнением к данным моделям является обширная база знаний MITRE ATT&CK. Ее применение позволяет осуществлять категоризацию и формиро-

вание поведенческих признаков нарушителя (APT) и производить поведенческую атрибуцию.

Чтобы минимизировать факторы постоянной эволюции APT и целевых атак, в ходе атрибуции необходимо применять новые методы и алгоритмы. Обогащение данных о киберугрозах и кибергруппировках, методы искусственного интеллекта и машинного обучения позволяют перейти от ручных методик к автоматизированным и повысить эффективность атрибуции при целевых атаках на КИИ.

Представленные методики атрибуции на основе аргументации и использования технических артефактов для выявления ложных флагов при атрибуции являются примерами реализуемых в настоящее время методик атрибуции кибернарушителей.

В последующих работах в рамках концепции многоуровневой атрибуции, планируется развить разработанные авторами настоящей статьи модели, алгоритмы и методики атрибуции, основанные на методах генерации и анализа графов атак [93, 94] и методах машинного, в том числе глубокого обучения [95, 96].

Рецензент: *Паращук Игорь Борисович, доктор технических наук, профессор, профессор Военной академии связи, Санкт-Петербург, Россия. E-mail: shchuk@rambler.ru*

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в Санкт-Петербургском Федеральном исследовательском центре Российской академии наук.

Литература

1. Stefano M. La strategia della Nato in ambito cyber / Mele Stefano // Europa Atlantica: [сайт] – URL: https://europaatlantica.it/firewall/2019/06/la-strategia-della-nato-in-ambito-cyber/ (дата обращения: 28.04.2022).
2. James S. Carbanak Threatens Critical Infrastructure: Cybercriminal APTs Merit Significant Investigation and Discussion / S. James. – Washington, DC, USA: ICIT, 2017. – 16 p.
3. Bulusu S.T., Laborde R., Wazan A.S., Barrère F., Benzekri A. Et al. Describing advanced persistent threats using a multi-agent system approach // 2017 1st cyber security in networking conference (CSNet). – IEEE, 2017. – P.1-3. – DOI: 10.1109/CSNET.2017.8241997.
4. Widiyasono N., Giriantari I.A.D., Sudarma M., Linawati L. Detection of Mirai Malware Attacks in IoT Environments Using Random Forest Algorithms / N. Widiyasono, I. A. D. Giriantari, M. Sudarma, L. Linawati // TEM Journal. Volume 10, Issue 3, P.1209-1219. – DOI: 10.18421/TEM103– 27.
5. McAfee Labs Threats Report // McAfee: [сайт] – URL: https://www.mcafee.com/enterprise/en–us/threat–center/mcafee–labs/reports.html (дата обращения: 28.04.2022).
6. Antonakakis M., April T., Bailey M., Bernhard M., Bursztein E., Cochran J., Zhou Y. et al. Understanding the mirai botnet // Proceedings of 26th USENIX security symposium (USENIX Security 17). – 2017. – P.1093-1110.
7. Eichensehr K.E. Decentralized cyberattack attribution / K.E. Eichensehr // American Journal of International Law. – 2019. – Volume 113. – P.213–217.
8. Tran D. The law of attribution: Rules for attribution the source of a cyber-attack / D Tran // Yale JL & Tech. – 2018. – Volume 20. – P. 376-411.
9. ACSC Releases Annual Cyber Threat Report for 2019–2020. CISA is part of the Department of Homeland Security: [сайт] – URL: https://us-cert.cisa.gov/ncas/current- activity/2020/09/10/acsc-releases-annual-cyber-threat-report-2019-2020 (дата обращения: 28.04.2022).
10. Актуальные киберугрозы: итоги 2020 года. Positive Technologies: [website] – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020 (дата обращения: 28.04.2022).
11. Серия отчетов Cisco по информационной безопасности. Cisco: [сайт] – URL: https://www.cisco.com/c/ru_ru/products/security/security-reports.html (дата обращения: 28.04.2022).
12. Edwards S. Effectively Testing APT Defences: Defining threats, addressing objections to testing and suggesting some practical approaches / S. Edwards, R. Ford, G. Szappanos. 2016 Virus Bulletin: [сайт] – URL: https://www.virusbulletin.com/virusbulletin/2016/01/paper-effectively-testing-apt-defences-defining-threats-addressing-objections-testing-and-suggesting-some-practical-approaches (дата обращения: 28.04.2022).
13. Chen P., Desmet L., Huygens C. A study on advanced persistent threats // IFIP International Conference on Communications and Multimedia Security. – Springer, Berlin, Heidelberg, 2014. – P.63-72. – DOI:10.1007/978– 3– 662– 44885– 4_5.hal– 01404186.
14. Edwards S., Ford R., Szappanos G. Effectively Testing APT Defences: Defining threats, addressing objections to testing and suggesting some practical approaches // Virus bulletin conference September. – 2015. P.291-299.
15. Clark R. M. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level / R. M. Clark, S. Hakim. Springer Cham, 2017. – 281 p. DOI: 10.1007/978-3-319-32824-9.
16. Интеллектуальные сервисы защиты информации в критических инфраструктурах / И.В. Котенко, И.Б. Саенко, Е.В. Дойникова [и др.]. – Санкт-Петербург: БХВ-Петербург, 2019. – 400 с.
17. Sood A. Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware / A. Sood, R. Enbody. Elsevier, USA, 2014. — 142 p.
18. Chen J. Special Issue on Advanced Persistent Threat / C. Jiageng, S. Chunhua, K.-H. Yeh, M. Yung // Future Generation Computer Systems. — 2018. — Vol.79. — P.243-246.

19. Robert M. L. The Problems with Seeking and Avoiding True Attribution to Cyber Attacks / M. L. Robert // Sans: [сайт]. — URL: https:// www.sans.org/blog/the– problems– with– seeking– and– avoiding– true– attribution– to– cyber– attacks (дата обращения: 28.04.2022).
20. Lemay A., Calvet J., Menet F., Fernandez J.M. Survey of publicly available reports on advanced persistent threat actors // Computers & Security. – 2018. Vol.72. P.26-59.
21. Hayes D. A Framework for More Effective Dark Web Marketplace Investigations / D. Hayes, Fr Cappa, J. Cardon // Information. – 2018. – 9 (8). –186. – 17 p. – DOI: 10.3390/info9080186.
22. Arnold N., Ebrahimi M., Zhang N., Lazarine B., Patton M., Chen H., Samtani S. Darknet ecosystem cyberthreat intelligence (CTI) tool // 2019 IEEE International Conference on Intelligence and Security Informatics (ISI). – IEEE, 2019. – P.92-97. – DOI:10.1109/ ISI.2019.8823501.
23. Eric M. H. The Cyber Kill Chain / M. H. Eric // Lockheed Martin Corporation: [сайт]. — URL: https://www.lockheedmartin.com/en– us/ capabilities/cyber/cyber– kill– chain.html (дата обращения: 28.04.2022).
24. Хмыров С.С., Котенко И.В. Анализ расширенной модели «cyber kill chain» для атрибуции нарушителей кибербезопасности при реализации целевых атак на объекты критической инфраструктуры // XII Санкт-Петербургская межрегиональная конференция ИБРР-2021. 2021. С.103-105.
25. Bahrami P. N. et al. Cyber kill chain-based taxonomy of advanced persistent threat actors: analogy of tactics, techniques, and procedures / P. N. Bahrami, A. Dehghantanha, T. Dargahi, R. M. Parizi, K. K. R. Choo, H. H Javadi // Journal of information processing systems. – 2019. – Vol. 15. – No.4. – P.865-889.
26. Kim H., Kwon H. J., Kim K. K. Modified cyber kill chain model for multimedia service environments // Multimedia Tools and Applications. – 2019. – Vol.78. – No.3. – P.3153-3170.
27. Siddiqi M. A., Ghani N. Critical analysis on advanced persistent threats // International Journal of Computer Applications. – 2016. – Vol.141. – No.13. – P.46-50. – DOI: 10.5120/ijca2016909784.
28. Bhatt P., Yano E. T., Gustavsson P. Towards a framework to detect multi– stage advanced persistent threats attacks // 2014 IEEE 8th international symposium on service-oriented system engineering. – IEEE, 2014. – P.390-395. – DOI: 10.1109/SOSE.2014.53.
29. Zhang R. et al. Constructing apt attack scenarios based on intrusion kill chain and fuzzy clustering // Security and Communication Networks. – 2017. – Vol. 2017. – Article ID 7536381, 9 p. – DOI: 10.1155/2017/7536381.
30. Hahn A. et al. A multi-layered and kill-chain based security analysis framework for cyber-physical systems // International Journal of Critical Infrastructure Protection. – 2015. – Vol.11. – P.39-50. – DOI: 10.1016/j.ijcip.2015.08.003.
31. Yadav T., Rao A. M. Technical aspects of cyber kill chain / T. Yadav, A.M. Rao // International Symposium on Security in Computing and Communication. (SSCC 2015). – Springer, Cham, 2015. – Vol.536. – P.438–452. – DOI: 10.1007/978– 3– 319– 22915– 7_40.
32. The Unified Kill Chain: [сайт]. – URL: https://unifiedkillchain.com/ (дата обращения: 28.04.2022).
33. Pols P. Modeling Fancy Bear Cyber Attacks: Designing a Unified Kill Chain for analyzing, comparing and defending against cyber-attacks / P. Pols // Leiden University. Student Repository: [сайт]. — URL: https://hdl.handle.net/1887/64569 (дата обращения: 28.04.2022).
34. Case D. U. Analysis of the cyber-attack on the Ukrainian power grid // Electricity Information Sharing and Analysis Center (E– ISAC). – 2016. –Vol.388. – P.1-29.
35. Dargahi T. et al. A cyber– kill– chain-based taxonomy of crypto– ransomware features // Journal of Computer Virology and Hacking Techniques. – 2019. – Vol.15. – No.4. – P.277– 305. – DOI: 10.1007/s11416– 019– 00338– 7.
36. Mackenzie P. WannaCry–Aftershock / P. Mackenzie // https://www.sophos.com: [сайт]. — URL: https://www.sophos.com/en-us/ medialibrary/PDFs/technical-papers/WannaCry-Aftershock.pdf (дата обращения: 28.04.2022).
37. Ahmed Y., Asyhari T., Rahman M.A. A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats // Computers, Materials and Continua. – 2021. – Vol.67. – No.2. – P.2497-2513. – DOI: 10.32604/cmc.2021.014223.
38. Aatiqah F.S., et al. A Cyber Kill Chain against APT attacks / F.S. Aatiqah, D. Menaga, G. Amarthiya, P. Divya // International Journal of Advanced Science and Technology. – 2020. – Vol.29. – No.10. – P.6899–6906.
39. Chu W.L., Lin C.J., Chang K.N. Detection and classification of advanced persistent threats and attacks using the support vector machine // Applied Sciences. – 2019. – Vol.9. – No.21. – 4579. – 16 p. – DOI: 10.3390/app9214579.
40. Hendler D., Kels S., Rubin A. Detecting malicious powershell commands using deep neural networks // Proceedings of the 2018 on Asia conference on computer and communications security. – 2018. – P.187-197. – DOI: 10.1145/3196494.3196511.
41. Li J., Cheng K., Wang S., Morstatter F., Trevino R.P., Tang J., Liu H. Feature selection: A data perspective / J.Li, K.Cheng, S.Wang, F.Morstatter, T.Morstatter, P.Robert, J.Tang, H.Liu // ACM computing surveys (CSUR). – 2017. – Vol.50. – No.6. – P.1-45. – DOI: 10.1145/3136625.
42. Ghafir I., Hammoudeh M., Prenosil V., Han L., Hegarty R., Rabie K., Aparicio-Navarro F.J. Detection of advanced persistent threat using machine learning correlation analysis / I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han, R. Hegarty, K. Rabie, F. J. Aparicio-Navarro // Future Generation Computer Systems. – 2018. – Vol.89. – P.349-359. – DOI: 10.1016/j.future.2018.06.055.
43. Kiwia D. et al. A cyber kill chain-based taxonomy of banking Trojans for evolutionary computational intelligence / D. Kiwia, A. Dehghantanha, K. K. R. Choo, J. Slaughter // Journal of computational science. – 2018. – Vol.27. – P.394–409. – DOI: 10.1016/j. jocs.2017.10.020.
44. Siddiqui S., Khan M. S., Ferens K., Kinsner, W. Detecting advanced persistent threats using fractal dimension based machine learning classification // Proceedings of the 2016 ACM on international workshop on security and privacy analytics. – 2016. – P.64-69. – DOI: 10.1145/2875475.2875484.
45. Wilkens F. et al. Multi-Stage Attack Detection via Kill Chain State Machines // Proceedings of the 3rd Workshop on Cyber– Security Arms Race. – 2021. – P.13-24. – DOI: 10.1145/3474374.3486918.
46. Milajerdi S. M. et al. Holmes: Real– Time APT Detection through Correlation of Suspicious Information Flows // 2019 IEEE Symposium on Security and Privacy (SP). – IEEE, 2019. – P.1137-1152. – DOI: 10.1109/SP.2019.00026.
47. Haas S., Fischer M. GAC: graph-based alert correlation for the detection of distributed multi– step attacks // Proceedings of the 33rd Annual ACM Symposium on Applied Computing. – 2018. – P.979– 988. – DOI: 10.1145/3167132.3167239.
48. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // ICISSp. – 2018. – Vol.1. – P.108-116. – DOI: 10.5220/0006639801080116.
49. Hossain M. N. et al. Dependence-Preserving Data Compaction for Scalable Forensic Analysis // 27th USENIX Security Symposium (USENIX Security 18). – 2018. – P.1723-1740.

50. Al-Mohannadi H. et al. Cyber-attack modeling analysis techniques: An overview // 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW). – IEEE, 2016. – P.69-76.
51. The Diamond Model of Intrusion Analysis / S. Caltagirone, A. Pendergast, C. Betz // www.threatintel.academy: [сайт]. — URL: https://www.threatintel.academy/wp-content/uploads/2020/07/diamond-model.pdf(дата обращения: 28.04.2022).
52. Mwiki H., Dargahi T., Dehghantanha A., Choo Raymond K.-K.R. Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin: Theories, Methods, Tools and Technologies // Critical Infrastructure Security and Resilience. – 2019. P.221-244. – DOI:10.1007/978-3-030-00024-0_12.
53. Kotheimer J., O'Meara K., Shick D. Using honeynets and the diamond model for ICS threat analysis. – Carnegie-Mellon Univ. Pittsburgh. CMU/SEI-2016-TR-006. CERT Division. 2016.
54. Skopik F., Pahi T. Under false flag: Using technical artifacts for cyber attack attribution // Cybersecurity. – 2020. – Vol. 3. – No.1. – P.1-20. – DOI:10.1186/s42400-020-00048-4
55. Treverton G. The intelligence challenges of hybrid threats: Focus on cyber and virtual realm. – Swedish Defence University. – 2018. – 36 p.
56. MITRE ATT&CK: Design and Philosophy // The MITRE Corporation: [сайт]. — URL: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf (дата обращения: 28.04.2022).
57. Best Practices for MITRE ATT&CK Mapping // www.cisa.gov: [сайт]. — URL: https://www.cisa.gov/uscert/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf (дата обращения: 28.04.2022).
58. Manocha H. et al. Security Assessment Rating Framework for Enterprises using MITRE ATT&CK Matrix // arXiv preprint arXiv:2108.06559. – 2021. – DOI: 10.48550/arXiv.2108.06559.
59. Aigner A., Khelil A. A Security Qualification Matrix to Efficiently Measure Security in Cyber– Physical Systems // 2020 32nd International Conference on Microelectronics (ICM). – IEEE, 2020. – P.1-4. – DOI: 10.1109/ICM50269.2020.9331797.
60. Aigner A., Khelil A. A Benchmark of Security Metrics in Cyber– Physical Systems // 2020 IEEE International Conference on Sensing, Communication and Networking (SECON Workshops). – IEEE, 2020. – P.1-6. – DOI: 10.1109/SECONWorkshops50264.2020.9149779.
61. Kim K. et al. Automatically Attributing Mobile Threat Actors by Vectorized ATT&CK Matrix and Paired Indicator / K. Kim, Y. Shin, J. Lee, K. Lee // Sensors. – 2021. – Vol.21. – No.19. – 6522. – 12 p. – DOI: 10.3390/s21196522.
62. Georgiadou A., Mouzakitis S., Askounis D. Assessing MITRE ATT& Risk Using a Cyber–Security Culture Framework // Sensors. – 2021. – Vol.21. – No.9. – 3267. – 14 p. – DOI: 10.3390/s21093267.
63. Securing the Extended Internet of Things (XIoT) // The Global State of Industrial Cybersecurity: [сайт]. — URL: https://claroty.com/ (дата обращения: 28.04.2022).
64. Bodeau D.J. et al. Cyber Threat Modeling: Survey, Assessment, and Representative Framework / D.J. Bodeau, C.D. McCollum, D. B. Fox // www.mitre.org: [сайт]. — URL: https://www.mitre.org/sites/default/ files/publications/pr_18– 1174– ngci– cyber– threat–modeling.pdf (дата обращения: 28.04.2022).
65. National Institute of Standards and Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0. February 12, 2014 / Institute of Standards and National // www.nist.gov: [сайт]. — URL: https://www.nist.gov/system/files/documents/cyberframework/cybersecurity– framework– 021214.pdf (дата обращения: 28.04.2022).
66. Friedman J., Bouchard M. Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks. – CyberEdge Group, 2015.
67. Seker E. Cyber Threat Intelligence Understanding Fundamentals. 2019. // https://www.researchgate.net: [сайт]. — URL: https://www.researchgate.net/publication/335692544_Cyber_Threat_Intelligence_ Understanding_Fundamentals (дата обращения: 28.06.2022).
68. Дойникова Е.В., Котенко И.В. Оценивание защищенности и выбор контрмер для управления кибербезопасностью. СПб.: Изд-во «Наука», 2021. – 197 с.
69. TAXII Version 2.0. Committee Specification 01 // oasis-open.org: [сайт]. — URL: https://docs.oasis– open.org/cti/taxii/v2.0/taxii–v2.0.html (дата обращения: 28.04.2022).
70. Papastergiou S., Mouratidis H., Kalogeraki E.M. Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures // Evolving Systems. – 2021. – Vol. 12. – No.1. – P.91-108. – DOI: 10.1007/s12530–020– 09335– 4.
71. Guercio, K. Top Threat Intelligence Platforms for 2022 / K. Guercio // www.esecurityplanet.com: [сайт]. — URL: https://www.esecurityplanet.com/products/threat-intelligence-platforms/ (дата обращения: 28.06.2022).
72. Gylling A. Enriching Attack Models with Cyber Threat Intelligence. Masters Theses / A. Gylling // Digitala Vetenskapliga Arkivet: [сайт]. — URL: http://kth.diva-portal.org/smash/get/diva2:1477504/ FULLTEXT01.pdf (дата обращения: 28.06.2022).
73. Noel L. RedAI: A Machine Learning Approach to Cyber Threat Intelligence. Masters Theses. 2020 // JMU Scholarly Commons: [сайт]. — URL: https://commons.lib.jmu.edu/cgi/ viewcontent.cgi?article=1093&context=masters202029 (дата обращения: 28.04.2022).
74. Sahrom A. M., Ariffin A., Selamat S. R., Yusof R. An Attribution of Cyberattack using Association Rule Mining (ARM) // International Journal of Advanced Computer Science and Applications (IJACSA). — 2020. – Vol. 11. – No. 2. – P.352-358.
75. Soldatos J., Philpot J., Giunta G. Cyber– Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber–Physical Protection of Modern Critical Infrastructures. – Now Publishers, 2020. – 450 p.
76. Securing machine learning algorithms / eds: A. Malatras, I. Agrafiotis, M. Adamczyk. European Union Agency for Cybersecurity (ENISA), 2021. — 70 p.
77. Ferrag M.A. et al. Deep learning techniques for cyber security intrusion detection: A detailed analysis // 6th International Symposium for ICS & SCADA Cyber Security Research 2019. – 2019. – P.126-136.
78. Ferrag M.A. et al. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study // Journal of Information Security and Applications. – 2020. – Vol. 50. – 102419.
79. Браницкий А.А., Котенко И.В. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейро-нечетких классификаторов // Информационно-управляющие системы, 2015, № 4 (77), С.69-77.
80. Гайфулина Д.А., Котенко И.В. Применение методов глубокого обучения в задачах кибербезопасности. Часть 1 // Вопросы кибербезопасности. 2020. №3(37). С 76-86. DOI: 10.21681/2311-3456-2020-03-76-86.
81. Гайфулина Д.А., Котенко И.В. Применение методов глубокого обучения в задачах кибербезопасности. Часть 2 // Вопросы кибер-

безопасности. 2020. № 4(38). С. 11-21. DOI: 10.21681/2311-3456-2020-04-11-21.
82. Eke H. N., Petrovski A., Ahriz H. The use of machine learning algorithms for detecting advanced persistent threats // Proceedings of the 12th International Conference on Security of Information and Networks. – 2019. – P. 1-8.
83. Brogi G. Real-time detection of Advanced Persistent Threats using Information Flow Tracking and Hidden Markov Models. Doctoral dissertation – Conservatoire national des arts et metiers. – CNAM, 2018.
84. Noor U. et al. A machine learning– based FinTech cyber threat attribution framework using high– level indicators of compromise / U. Noor, Z. Anwar, T. Amjad, K. K. R. Choo // Future Generation Computer Systems. – 2019. – Vol. 96. – P.227-242.
85. Karafili E., Wang L., Lupu E. C. An argumentation-based reasoner to assist digital investigation and attribution of cyber-attacks // Forensic Science International: Digital Investigation. – 2020. – Vol. 32. – 300925.
86. Skopik F., Timea P. Under false flag: using technical artifacts for cyber attack attribution // Cybersecurity, 2020. Vol.8, No 3. 20 p.
87. Thomas R., Buchanan B. Attributing Cyber Attacks // Journal of Strategic Studies, 38: 1-2, 2015. P.4-37.
88. Global cybersecurity Index (GCI). International Telecommunication Union [сайт]. — URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (дата обращения: 05.05.2022).
89. Breene K. Who are the cyberwar superpowers?: [сайт]. — URL: http://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers (дата обращения: 05.05.2022).
90. Kakas A., Moraitis P. Argumentation based decision making for autonomous agents // Proceedings of the second international joint conference on Autonomous agents and multiagent systems (AAMAS '03), 2003. P. 883-890.
91. Morgan R., Kelly D. A novel perspective on cyber attribution // 14th International Conference on Cyber Warfare and Security (ICCWS), 2019. 11 p.
92. Chiesa R., Ducci S., & Ciappi S. Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking. Auerbach Publications, 2008, 279 p.
93. Kotenko I., Doynikova E. Security Assessment of Computer Networks based on Attack Graphs and Security Events // Lecture Notes in Computer Science. 2014. Vol.8407. P.462-471.
94. Kotenko I., Chechulin A. Computer Attack Modeling and Security Evaluation based on Attack Graphs // Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS 2013. 2013. С. 614-619.
95. Doynikova E., Novikova E., Gaifulina D., Kotenko I. Towards Attacker Attribution for Risk Analysis // Risks and Security of Internet and Systems – 15th International Conference, CRiSIS 2020, Paris, France, November 4-6, 2020, Revised Selected Papers. Lecture Notes in Computer Science, 12528. Joaquin Garcia-Alfaro, Jean Leneutre, Nora Cuppens, Reda Yaich (Eds.), Springer 2021, ISBN 978-3-030-68886-8. P.347-353.
96. Котенко И.В., Хмыров С.С. Анализ актуальных методик атрибуции нарушителей кибербезопасности при реализации целевых атак на объекты критической инфраструктуры // Юбилейная X Международная научно-техническая и научно-методическая конференция "Актуальные проблемы инфотелекоммуникаций в науке и образовании" (АПИНО-2021). 2021. СПб.: СПбГУТ, 2021. Том 1. С.536-541.

ANALYSIS OF MODELS AND TECHNIQUES USED FOR ATTRIBUTION OF CYBER SECURITY VIOLATORS IN THE IMPLEMENTATION OF TARGETED ATTACKS

Kotenko I.V. [3]***, Khmyrov S.S.*** [4]

Purpose of the paper: *analysis of models and techniques used for attribution of cybersecurity violators in the interests of building a promising attribution system in the implementation of targeted attacks against critical information infrastructure objects.*

Research method: *system analysis of open sources of data on the attribution of cyber-violators in the implementation of targeted attacks against critical information infrastructure objects over a period mainly over the last 5 years.*

The result obtained: *based on the consideration of open sources, the paper presents an analysis of the models and techniques used to attribute cyber intruders in the implementation of targeted attacks and used both in scientific and practical projects. The paper analyzes new models used for attribution, allowing the collection of data at the tactical-technical and socio-political levels. The main indicators of ongoing cyber attacks and intruders that are essential for the implementation of attribution processes are identified. The procedure for generating data for*

3 Igor V. Kotenko, Dr.Sc., Professor, Chief Scientist and Head of Laboratory of Computer Security Problems at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: ivkote@comsec.spb.ru

4 Semyon S. Khmyrov, Ph.D. Student at St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. E-mail: khmyrov.s.s@gmail.com

profiling cybergroups is considered, as well as the possibility of using the considered models and techniques in the interests of building a promising system for attribution of a cyber intruder in the implementation of targeted attacks against critical information infrastructure objects. The analysis was carried out according to sources over a twenty-year period, meanwhile, the main works under consideration were published in the last 5 years. The analysis does not claim to be complete, but an attempt is made to cover the most significant studies.

***Scientific novelty** lies in the fact that the presented paper is one of the first domestic works that provides a detailed analysis of studies published in recent years in the field of attribution of cyber security violators. Models such as «cyber intrusion chain», «unified cyber intrusion chain», Diamond basic and extended intrusion analysis models, ATT&CK model are considered. Examples of attribution methods for argumentation-based reasoning with evidence at the technical and social levels and the use of technical artifacts to identify false flags in attribution are given. Besides, the paper also lists trends in the usage of modern solutions for detecting and attributing attacks based on artificial intelligence and machine learning.*

***Keywords:** cyber attack, cyber operation, critical infrastructure, artificial intelligence, machine learning, advanced persistent threat, intrusion detection, intruder profiling, cyber kill chain.*

References

1. Stefano M. La strategia della Nato in ambito cyber / Mele Stefano // Europa Atlantica: [website] – URL: https://europaatlantica.it/firewall/2019/06/la-strategia-della-nato-in-ambito-cyber/ (date of access: 28.04.2022).
2. James S. Carbanak Threatens Critical Infrastructure: Cybercriminal APTs Merit Significant Investigation and Discussion / S. James. – Washington, DC, USA: ICIT, 2017. – 16 p.
3. Bulusu S.T., Laborde R., Wazan A.S., Barrère F., Benzekri A. Et al. Describing advanced persistent threats using a multi-agent system approach // 2017 1st cyber security in networking conference (CSNet). – IEEE, 2017. – P.1-3. – DOI: 10.1109/CSNET.2017.8241997.
4. Widiyasono N., Giriantari I.A.D., Sudarma M., Linawati L. Detection of Mirai Malware Attacks in IoT Environments Using Random Forest Algorithms / N. Widiyasono, I. A. D. Giriantari, M. Sudarma, L. Linawati // TEM Journal. Volume 10, Issue 3, P.1209-1219. – DOI: 10.18421/TEM103– 27.
5. McAfee Labs Threats Report // McAfee: [website] – URL: https://www.mcafee.com/enterprise/en–us/threat–center/mcafee–labs/reports.html (date of access: 28.04.2022).
6. Antonakakis M., April T., Bailey M., Bernhard M., Bursztein E., Cochran J., Zhou Y. et al. Understanding the mirai botnet // Proceedings of 26th USENIX security symposium (USENIX Security 17). 2017. – P.1093-1110.
7. Eichensehr K.E. Decentralized cyberattack attribution / K.E. Eichensehr // American Journal of International Law. – 2019. – Volume 113. – P.213–217.
8. Tran D. The law of attribution: Rules for attribution the source of a cyber-attack / D Tran // Yale JL & Tech. – 2018. – Volume 20. – P. 376-411.
9. ACSC Releases Annual Cyber Threat Report for 2019–2020. CISA is part of the Department of Homeland Security: [website] – URL: https://us-cert.cisa.gov/ncas/current- activity/2020/09/10/acsc-releases-annual-cyber-threat-report-2019-2020 (date of access: 28.04.2022).
10. Actual cyber threats: results of 2020. Positive Technologies: [website] – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020 (date of access: 28.04.2022).
11. Cisco Security Report Series. Cisco: [website] – URL: https://www.cisco.com/c/ru_ru/products/security/security-reports.html (date of access: 28.04.2022).
12. Edwards S. Effectively Testing APT Defences: Defining threats, addressing objections to testing and suggesting some practical approaches / S. Edwards, R. Ford, G. Szappanos. 2016 Virus Bulletin: [website] – URL: https://www.virusbulletin.com/virusbulletin/2016/01/paper- effectively-testing-apt-defences-defining-threats-addressing-objections-testing-and-suggesting-some-practical-approaches (date of access: 28.04.2022).
13. Chen P., Desmet L., Huygens C. A study on advanced persistent threats // IFIP International Conference on Communications and Multimedia Security. – Springer, Berlin, Heidelberg, 2014. – P.63-72. – DOI:10.1007/978– 3– 662– 44885– 4_5.hal– 01404186.
14. Edwards S., Ford R., Szappanos G. Effectively Testing APT Defences: Defining threats, addressing objections to testing and suggesting some practical approaches // Virus bulletin conference September. – 2015. P.291-299.
15. Clark R. M. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level / R. M. Clark, S. Hakim. Springer Cham, 2017. – 281 p. DOI: 10.1007/978-3-319-32824-9.
16. Intelligent information security services in critical infrastructures / I.V. Kotenko, I.B. Saenko, E.V. Doynikova [et al.]. – St. Petersburg: BHV-Petersburg, 2019. – 400 p. (in Russian).
17. Sood A. Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware / A. Sood, R. Enbody. Elsevier, USA, 2014. — 142 p.
18. Chen J. Special Issue on Advanced Persistent Threat / C. Jiageng, S. Chunhua, K.-H. Yeh, M. Yung // Future Generation Computer Systems. — 2018. — Vol.79. — P.243-246.
19. Robert M. L. The Problems with Seeking and Avoiding True Attribution to Cyber Attacks / M. L. Robert // Sans: [website]. — URL: https://www.sans.org/blog/the– problems– with– seeking– and– avoiding– true– attribution– to– cyber– attacks (date of access: 28.04.2022).
20. Lemay A., Calvet J., Menet F., Fernandez J.M. Survey of publicly available reports on advanced persistent threat actors // Computers & Security. – 2018. Vol.72. P.26-59.
21. Hayes D. A Framework for More Effective Dark Web Marketplace Investigations / D. Hayes, Fr Cappa, J. Cardon // Information. – 2018. – 9 (8). –186. – 17 p. – DOI: 10.3390/info9080186.

22. Arnold N., Ebrahimi M., Zhang N., Lazarine B., Patton M., Chen H., Samtani S. Darknet ecosystem cyberthreat intelligence (CTI) tool // 2019 IEEE International Conference on Intelligence and Security Informatics (ISI). – IEEE, 2019. – P.92-97. – DOI:10.1109/ISI.2019.8823501.
23. Eric M. H. The Cyber Kill Chain / M. H. Eric // Lockheed Martin Corporation: [website]. — URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber- kill- chain.html (date of access: 28.04.2022).
24. Khmyrov S.S., Kotenko I.V. Analysis of the extended "cyber kill chain" model for attribution of cybersecurity violators in the implementation of targeted attacks on critical infrastructure objects // XII St. Petersburg Interregional Conference of the IBRR-2021. 2021. P.103-105 (in Russian).
25. Bahrami P. N. et al. Cyber kill chain-based taxonomy of advanced persistent threat actors: analogy of tactics, techniques, and procedures / P. N. Bahrami, A. Dehghantanha, T. Dargahi, R. M. Parizi, K. K. R. Choo, H. H Javadi // Journal of information processing systems. – 2019. – Vol. 15. – No.4. – P.865-889.
26. Kim H., Kwon H. J., Kim K. K. Modified cyber kill chain model for multimedia service environments // Multimedia Tools and Applications. – 2019. – Vol.78. – No.3. – P.3153-3170.
27. Siddiqi M. A., Ghani N. Critical analysis on advanced persistent threats // International Journal of Computer Applications. – 2016. – Vol.141. – No.13. – P.46-50. – DOI: 10.5120/ijca2016909784.
28. Bhatt P., Yano E. T., Gustavsson P. Towards a framework to detect multi- stage advanced persistent threats attacks // 2014 IEEE 8th international symposium on service oriented system engineering. – IEEE, 2014. – P.390-395. – DOI: 10.1109/SOSE.2014.53.
29. Zhang R. et al. Constructing apt attack scenarios based on intrusion kill chain and fuzzy clustering // Security and Communication Networks. – 2017. – Vol. 2017. – Article ID 7536381, 9 p. – DOI: 10.1155/2017/7536381.
30. Hahn A. et al. A multi-layered and kill-chain based security analysis framework for cyber-physical systems // International Journal of Critical Infrastructure Protection. – 2015. – Vol.11. – P.39-50. – DOI: 10.1016/j.ijcip.2015.08.003.
31. Yadav T., Rao A. M. Technical aspects of cyber kill chain / T. Yadav, A.M. Rao // International Symposium on Security in Computing and Communication. (SSCC 2015). – Springer, Cham, 2015. – Vol.536. – P.438–452. – DOI: 10.1007/978- 3- 319- 22915- 7_40.
32. The Unified Kill Chain: [website]. – URL: https://unifiedkillchain.com/ (date of access: 28.04.2022).
33. Pols P. Modeling Fancy Bear Cyber Attacks: Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks / P. Pols // Leiden University. Student Repository: [website]. — URL: https://hdl.handle.net/1887/64569 (date of access: 28.04.2022).
34. Case D. U. Analysis of the cyber attack on the Ukrainian power grid // Electricity Information Sharing and Analysis Center (E- ISAC). – 2016. –Vol.388. – P.1-29.
35. Dargahi T. et al. A cyber- kill- chain based taxonomy of crypto- ransomware features // Journal of Computer Virology and Hacking Techniques. – 2019. – Vol.15. – No.4. – P.277- 305. – DOI: 10.1007/s11416- 019- 00338- 7.
36. Mackenzie P. WannaCry–Aftershock / P. Mackenzie // https://www.sophos.com: [website]. — URL: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/WannaCry-Aftershock.pdf (date of access: 28.04.2022).
37. Ahmed Y., Asyhari T., Rahman M.A. A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats // Computers, Materials and Continua. – 2021. – Vol.67. – No.2. – P.2497-2513. – DOI: 10.32604/cmc.2021.014223.
38. Aatiqah F.S., et al. A Cyber Kill Chain against APT attacks / F.S. Aatiqah, D. Menaga, G. Amarthiya, P. Divya // International Journal of Advanced Science and Technology. – 2020. – Vol.29. – No.10. – P.6899–6906.
39. Chu W.L., Lin C.J., Chang K.N. Detection and classification of advanced persistent threats and attacks using the support vector machine // Applied Sciences. – 2019. – Vol.9. – No.21. – 4579. – 16 p. – DOI: 10.3390/app9214579.
40. Hendler D., Kels S., Rubin A. Detecting malicious powershell commands using deep neural networks // Proceedings of the 2018 on Asia conference on computer and communications security. – 2018. – P.187-197. – DOI: 10.1145/3196494.3196511.
41. Li J., Cheng K., Wang S., Morstatter F., Trevino R.P., Tang J., Liu H. Feature selection: A data perspective / J.Li, K.Cheng, S.Wang, F.Morstatter, T.Morstatter, P.Robert, J.Tang, H.Liu // ACM computing surveys (CSUR). – 2017. – Vol.50. – No.6. – P.1-45. – DOI: 10.1145/3136625.
42. Ghafir I., Hammoudeh M., Prenosil V., Han L., Hegarty R., Rabie K., Aparicio-Navarro F.J. Detection of advanced persistent threat using machine learning correlation analysis / I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han, R. Hegarty, K. Rabie, F. J. Aparicio-Navarro // Future Generation Computer Systems. – 2018. – Vol.89. – P.349-359. – DOI: 10.1016/j.future.2018.06.055.
43. Kiwia D. et al. A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence / D. Kiwia, A. Dehghantanha, K. K. R. Choo, J. Slaughter // Journal of computational science. – 2018. – Vol.27. – P.394–409. – DOI: 10.1016/j.jocs.2017.10.020.
44. Siddiqui S., Khan M. S., Ferens K., Kinsner, W. Detecting advanced persistent threats using fractal dimension based machine learning classification // Proceedings of the 2016 ACM on international workshop on security and privacy analytics. – 2016. – P.64-69. – DOI: 10.1145/2875475.2875484.
45. Wilkens F. et al. Multi-Stage Attack Detection via Kill Chain State Machines // Proceedings of the 3rd Workshop on Cyber- Security Arms Race. – 2021. – P.13-24. – DOI: 10.1145/3474374.3486918.
46. Milajerdi S. M. et al. Holmes: Real- Time APT Detection through Correlation of Suspicious Information Flows // 2019 IEEE Symposium on Security and Privacy (SP). – IEEE, 2019. – P.1137-1152. – DOI: 10.1109/SP.2019.00026.
47. Haas S., Fischer M. GAC: graph-based alert correlation for the detection of distributed multi- step attacks // Proceedings of the 33rd Annual ACM Symposium on Applied Computing. – 2018. – P.979- 988. – DOI: 10.1145/3167132.3167239.
48. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // ICISSp. – 2018. – Vol.1. – P.108-116. – DOI: 10.5220/0006639801080116.
49. Hossain M. N. et al. Dependence-Preserving Data Compaction for Scalable Forensic Analysis // 27th USENIX Security Symposium (USENIX Security 18). – 2018. – P.1723-1740.
50. Al-Mohannadi H. et al. Cyber-attack modeling analysis techniques: An overview // 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW). – IEEE, 2016. – P.69-76.
51. The Diamond Model of Intrusion Analysis / S. Caltagirone, A. Pendergast, C. Betz // www.threatintel.academy: [website]. — URL: https://www.threatintel.academy/wp-content/uploads/2020/07/diamond-model.pdf(date of access: 28.04.2022).
52. Mwiki H., Dargahi T., Dehghantanha A., Choo Raymond K.-K.R. Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin: Theories, Methods, Tools and Technologies // Critical Infrastructure Security and Resilience. – 2019. P.221-244. – DOI:10.1007/978-3-030-00024-0_12.

53. Kotheimer J., O'Meara K., Shick D. Using honeynets and the diamond model for ICS threat analysis. – Carnegie-Mellon Univ. Pittsburgh. CMU/SEI-2016-TR-006. CERT Division. 2016.
54. Skopik F., Pahi T. Under false flag: Using technical artifacts for cyber attack attribution // Cybersecurity. – 2020. – Vol. 3. – No.1. – P.1-20. – DOI:10.1186/s42400-020-00048-4
55. Treverton G. The intelligence challenges of hybrid threats: Focus on cyber and virtual realm. – Swedish Defence University. – 2018. – 36 p.
56. MITRE ATT&CK: Design and Philosophy // The MITRE Corporation: [website]. — URL: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf (date of access: 28.04.2022).
57. Best Practices for MITRE ATT&CK Mapping // www.cisa.gov: [website]. — URL: https://www.cisa.gov/uscert/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf (date of access: 28.04.2022).
58. Manocha H. et al. Security Assessment Rating Framework for Enterprises using MITRE ATT&CK Matrix // arXiv preprint arXiv:2108.06559. – 2021. – DOI: 10.48550/arXiv.2108.06559.
59. Aigner A., Khelil A. A Security Qualification Matrix to Efficiently Measure Security in Cyber– Physical Systems // 2020 32nd International Conference on Microelectronics (ICM). – IEEE, 2020. – P.1-4. – DOI: 10.1109/ICM50269.2020.9331797.
60. Aigner A., Khelil A. A Benchmark of Security Metrics in Cyber– Physical Systems // 2020 IEEE International Conference on Sensing, Communication and Networking (SECON Workshops). – IEEE, 2020. – P.1-6. – DOI: 10.1109/SECONWorkshops50264.2020.9149779.
61. Kim K. et al. Automatically Attributing Mobile Threat Actors by Vectorized ATT&CK Matrix and Paired Indicator / K. Kim, Y. Shin, J. Lee, K. Lee // Sensors. – 2021. – Vol.21. – No.19. – 6522. – 12 p. – DOI: 10.3390/s21196522.
62. Georgiadou A., Mouzakitis S., Askounis D. Assessing MITRE ATT& Risk Using a Cyber–Security Culture Framework // Sensors. – 2021. – Vol.21. – No.9. – 3267. – 14 p. – DOI: 10.3390/s21093267.
63. Securing the Extended Internet of Things (XIoT) // The Global State of Industrial Cybersecurity: [website]. — URL: https://claroty.com/ (date of access: 28.04.2022).
64. Bodeau D.J. et al. Cyber Threat Modeling: Survey, Assessment, and Representative Framework / D.J. Bodeau, C.D. McCollum, D. B. Fox // www.mitre.org: [website]. — URL: https://www.mitre.org/sites/default/ files/publications/pr_18– 1174– ngci– cyber– threat–modeling.pdf (date of access: 28.04.2022).
65. National Institute of Standards and Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0. February 12, 2014 / Institute of Standards and National // www.nist.gov: [website]. — URL: https://www.nist.gov/system/files/documents/cyberframework/cybersecurity– framework– 021214.pdf (date of access: 28.04.2022).
66. Friedman J., Bouchard M. Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks. – CyberEdge Group, 2015.
67. Seker E. Cyber Threat Intelligence Understanding Fundamentals. 2019. // https://www.researchgate.net: [website]. — URL: https://www.researchgate.net/publication/335692544_Cyber_Threat_Intelligence_ Understanding_Fundamentals (date of access: 28.06.2022).
68. Doynikova E.V., Kotenko I.V. Assessment of security and countermeasure selection for cybersecurity management. St. Petersburg: Publishing house "Science", 2021. – 197 p. (in Russian).
69. TAXII Version 2.0. Committee Specification 01 // oasis-open.org: [website]. — URL: https://docs.oasis– open.org/cti/taxii/v2.0/taxii–v2.0.html (date of access: 28.04.2022).
70. Papastergiou S., Mouratidis H., Kalogeraki E.M. Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures // Evolving Systems. – 2021. – Vol. 12. – No.1. – P.91-108. – DOI: 10.1007/s12530–020– 09335– 4.
71. Guercio, K. Top Threat Intelligence Platforms for 2022 / K. Guercio // www.esecurityplanet.com: [website]. — URL: https://www.esecurityplanet.com/products/threat-intelligence-platforms/ (date of access: 28.06.2022).
72. Gylling A. Enriching Attack Models with Cyber Threat Intelligence. Masters Theses / A. Gylling // Digitala Vetenskapliga Arkivet: [website]. — URL: http://kth.diva-portal.org/smash/get/diva2:1477504/ FULLTEXT01.pdf (date of access: 28.06.2022).
73. Noel L. RedAl: A Machine Learning Approach to Cyber Threat Intelligence. Masters Theses. 2020 // JMU Scholarly Commons: [website]. — URL: https://commons.lib.jmu.edu/cgi/ viewcontent.cgi?article=1093&context=masters202029 (date of access: 28.04.2022).
74. Sahrom A. M., Ariffin A., Selamat S. R., Yusof R. An Attribution of Cyberattack using Association Rule Mining (ARM) // International Journal of Advanced Computer Science and Applications (IJACSA). — 2020. – Vol. 11. – No. 2. – P.352-358.
75. Soldatos J., Philpot J., Giunta G. Cyber– Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber–Physical Protection of Modern Critical Infrastructures. – Now Publishers, 2020. – 450 p.
76. Securing machine learning algorithms / eds: A. Malatras, I. Agrafiotis, M. Adamczyk. European Union Agency for Cybersecurity (ENISA), 2021. — 70 p.
77. Ferrag M.A. et al. Deep learning techniques for cyber security intrusion detection: A detailed analysis // 6th International Symposium for ICS & SCADA Cyber Security Research 2019. – 2019. – P.126-136.
78. Ferrag M.A. et al. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study // Journal of Information Security and Applications. – 2020. – Vol. 50. – 102419.
79. Branitsky A.A., Kotenko I.V. Detection of network attacks based on the integration of neural, immune and neuro-fuzzy classifiers // Information and control systems, 2015, No. 4 (77), P.69-77 (in Russian).
80. Gaifullina D.A., Kotenko I.V. Application of deep learning methods in cybersecurity tasks. Part 1 // Cybersecurity issues. 2020. №3(37). P.76-86. DOI: 10.21681/2311-3456-2020-03-76-86 (in Russian).
81. Gaifullina D.A., Kotenko I.V. Application of deep learning methods in cybersecurity tasks. Part 2 // Cybersecurity issues. 2020. No. 4(38). pp. 11-21. DOI: 10.21681/2311-3456-2020-04-11-21 (in Russian).
82. Eke H. N., Petrovski A., Ahriz H. The use of machine learning algorithms for detecting advanced persistent threats // Proceedings of the 12th International Conference on Security of Information and Networks. – 2019. – P. 1-8.
83. Brogi G. Real-time detection of Advanced Persistent Threats using Information Flow Tracking and Hidden Markov Models. Doctoral dissertation – Conservatoire national des arts et metiers. – CNAM, 2018.
84. Noor U. et al. A machine learning– based FinTech cyber threat attribution framework using high– level indicators of compromise / U. Noor, Z. Anwar, T. Amjad, K. K. R. Choo // Future Generation Computer Systems. – 2019. – Vol. 96. – P.227-242.

85. Karafili E., Wang L., Lupu E. C. An argumentation-based reasoner to assist digital investigation and attribution of cyber-attacks // Forensic Science International: Digital Investigation. – 2020. – Vol. 32. – 300925.
86. Skopik F., Timea P. Under false flag: using technical artifacts for cyber attack attribution // Cybersecurity, 2020. Vol.8, No 3. 20 p.
87. Thomas R., Buchanan B. Attributing Cyber Attacks // Journal of Strategic Studies, 38: 1-2, 2015. P.4-37.
88. Global cybersecurity Index (GCI). International Telecommunication Union [website]. — URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (date of access: 05.05.2022).
89. Breene K. Who are the cyberwar superpowers?: [website]. — URL: http://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers (date of access: 05.05.2022).
90. Kakas A., Moraitis P. Argumentation based decision making for autonomous agents // Proceedings of the second international joint conference on Autonomous agents and multiagent systems (AAMAS '03), 2003. P. 883-890.
91. Morgan R., Kelly D. A novel perspective on cyber attribution // 14th International Conference on Cyber Warfare and Security (ICCWS), 2019. 11 p.
92. Chiesa R., Ducci S., & Ciappi S. Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking. Auerbach Publications, 2008, 279 p.
93. Kotenko I., Doynikova E. Security Assessment of Computer Networks based on Attack Graphs and Security Events // Lecture Notes in Computer Science. 2014. Vol.8407. P.462-471.
94. Kotenko I., Chechulin A. Computer Attack Modeling and Security Evaluation based on Attack Graphs // Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS 2013. 2013. С. 614-619.
95. Doynikova E., Novikova E., Gaifulina D., Kotenko I. Towards Attacker Attribution for Risk Analysis // Risks and Security of Internet and Systems – 15th International Conference, CRiSIS 2020, Paris, France, November 4-6, 2020, Revised Selected Papers. Lecture Notes in Computer Science, 12528. Joaquin Garcia-Alfaro, Jean Leneutre, Nora Cuppens, Reda Yaich (Eds.), Springer 2021, ISBN 978-3-030-68886-8. P.347-353.
96. Kotenko I.V., Khmyrov S.S. Analysis of current methods of attribution of cybersecurity violators in the implementation of targeted attacks on critical infrastructure objects // 10th International Conference on Advanced Infotelecommunications (ICAIT 2021)2021. St. Petersburg: SPbGUT, 2021. Vol.1. P.536-541 (in Russian).