КОГНИТИВНОЕ МОДЕЛИРОВАНИЕ ВЕКТОРА КИБЕРАТАК НА ОСНОВЕ МЕТАШАБЛОНОВ CAPEC

***Васильев В.И.*[1], *Кириллова А.Д.* [2], *Вульфин А.М.* [3]**

Цель исследования: *автоматизация моделирования вектора сложной атаки на основе формализованных меташаблонов CAPEC*[4] *в базисе нечетких когнитивных карт.*

Метод исследования: *моделирование вектора атаки в виде графа атак с дальнейшей формализацией в виде иерархической нечеткой когнитивной карты для возможности анализа с требуемым уровнем детализации и количественной оценки рисков кибербезопасности.*

Полученные результаты: *предложен сценарный подход к моделированию сложных многошаговых целенаправленных кибератак на основе проекта Методики моделирования угроз безопасности ФСТЭК России и базы меташаблонов атак CAPEC. Алгоритм «сворачивания» детализированной нечеткой когнитивной карты вектора атаки показан на примере угрозы перехвата управления автоматизированной системы управления технологическими процессами нефтедобывающего предприятия с оценкой вероятности реализации с учетом уровня опасности эксплуатируемых уязвимостей. Разработаны основные программные модули системы. Проведены вычислительные эксперименты с целью оценки эффективности ее применения. Показано, что в результате анализа вектора кибератак в нечетком когнитивном базисе эксперт может ранжировать возможные сценарии реализации с учетом используемых уязвимостей, оценить уровень опасности реализации каждого сценария в отдельности и кибератаки в целом.*

Ключевые слова: *нечеткая когнитивная карта, оценка рисков, граф атак, сценарий, шаблон атаки, уязвимости, эшелонированная защита.*

DOI: 10.21681/2311-3456-2021-2-2-16

Введение

Цифровизация производства ведет к сопряжению технологических и корпоративных сегментов инфраструктуры предприятия, что неизбежно влечет за собой уменьшение степени изоляции автоматизированных систем управления технологическими процессами (АСУ ТП). Согласно исследованиям Positive Technologies, в III квартале 2020 года выявлено на 2,7% больше атак на промышленные системы по сравнению со II кварталом и на 54% по сравнению с аналогичным периодом 2019 года. По данным компании Clatory, свыше 70% выявленных в I полугодии 2020 года уязвимостей допускают удаленную эксплуатацию, и основным является сетевой вектор атаки. Доля уязвимостей компонентов АСУ ТП, используемых при реализации локального вектора атак, увеличилась на 8,6% по сравнению с I полугодием 2019 года.

Современные атаки значительно отличаются от того, какими они были десять лет назад. Сегодня преобладают многошаговые скоординированные распределенные атаки со сложной организацией, сложным процессом реализации, множеством целей (APT, advanced persistent threats) [1, 2]. В подобном ландшафте угроз при обеспечении кибербезопасности объектов информационной инфраструктуры на первый план выдвигается создание интеллектуальных средств защиты, позволяющих обнаруживать сложные целевые атаки еще на начальных этапах их реализации, опираясь на множество индикаторов компрометации (IOC, Indicator of Compromise) и индикаторы атак (IOA, Indicator of Attack). Подобные индикаторы позволяют описывать отдельные вредоносные объекты, действия или подозрительное поведение системы, при совпадении с ними события кибербезопасности помечаются как потенциальные элементы атаки. При сопоставлении IOC с IOA основным инструментом становится моделирование вектора атаки на различных этапах ее жизненного цикла: обнаружение уже совершенных вредоносных действий злоумышленника, определение значимости и устранение последствий, формирование рекомендаций для предотвращения возникновения инцидентов в будущем. Построение вектора атаки без применения средств компьютерной автоматизации трудоемко и требует наличия высококвалифицированных специалистов. Для решения данной проблемы предлагается ав-

1 Васильев Владимир Иванович, доктор технических наук, профессор, профессор кафедры вычислительной техники и защиты информации Уфимского государственного авиационного технического университета, г. Уфа, Россия. E-mail: vasilyev@ugatu.ac.ru

2 Кириллова Анастасия Дмитриевна, аспирант кафедры вычислительной техники и защиты информации Уфимского государственного авиационного технического университета, г. Уфа, Россия. E-mail: kirillova.andm@gmail.com

3 Вульфин Алексей Михайлович, кандидат технических наук, доцент кафедры вычислительной техники и защиты информации Уфимского государственного авиационного технического университета, г. Уфа, Россия. E-mail: vulfin.alexey@gmail.com

4 CAPEC - Common Attack Pattern Enumeration and Classification

томатизировать процесс моделирования вектора атаки на основе формализованных меташаблонов в базисе нечетких когнитивных карт (НКК). Это позволит выбирать требуемый в процессе анализа уровень детализации вектора атаки, доводя решение до количественных оценок локального относительного риска, основываясь на метриках оценки опасности CVSS уязвимостей и недостатков программного, аппаратного и организационного обеспечения.

1. Анализ методик моделирования вектора кибератаки

В общем случае кибератака представляет собой набор последовательных действий, включающих в себя комплекс мероприятий и воздействий, приближающих нарушителя к достижению цели. Одной из наиболее известных методик в области анализа кибератак является методика, основанная на моделировании сценариев их реализации на основе модели Cyber Kill Chain [3, 4].

Весной 2020 года ФСТЭК России опубликовал проект Методики моделирования угроз безопасности информации [5], ориентированной на определение актуальных угроз безопасности информации, где каждый инцидент рассматривается как набор последовательных действий злоумышленника в рамках некоторого сценария. В результате определяется уровень опасности каждой угрозы безопасности информации для каждого из сценариев реализации угроз для разработки перечня актуальных угроз. Для определения всех возможных сценариев атаки предлагается использовать приведенные в Методике тактики и техники, а также дополнительную информацию из банка данных угроз безопасности информации (БДУ) ФСТЭК или других баз данных компьютерных атак. На сегодняшний день основными инструментами для моделирования атак являются базы данных компании MITRE, как наиболее систематизированные источники информации о действиях злоумышленника.

База данных MITRE ATT&CK [6] представляет собой совокупность техник, которые группируются в тактики, направленные на достижение злоумышленником конечной или промежуточной цели. В отличие от тактик и техник из проекта Методики, приведенные в ATT&CK тактики подробно описывают возможные варианты поведения злоумышленника, для каждой техники представлено подробное описание и известные случаи применения, а также методы обнаружения и потенциальные меры по нейтрализации атаки. Таким образом, база данных ATT&CK позволяет детально проанализировать действия злоумышленника при моделировании кибератаки [7, 8].

Для более полного рассмотрения всех возможных шагов злоумышленников компанией MITRE был разработан стандарт CAPEC (Common Attack Pattern Enumeration and Classification) [9-11], включающий в себя перечень и классификатор шаблонов типовых атак, т.е. описание общих методов, используемых при атаках на уязвимые компоненты информационной системы. Каталог в CAPEC представляет собой набор меташаблонов атак, сгруппированных по некоторым общим критериям. Меташаблон атаки – абстрактная характеристика конкретной методологии или техники, используемой в атаке.

Отметим, что хотя БДУ ФСТЭК во многом схожа с базой шаблонов атак CAPEC, она все же не имеет структурированной таксономии и не дает четкого понимания о том, как реализуется та или иная угроза. Кроме того, при использовании БДУ ФСТЭК нет возможности перейти от общетеоретического и высокоуровневого описания угрозы на уровень оценки конкретных действий злоумышленника при ее реализации.

В связи с этим представляется необходимым, в дополнение к Методике ФСТЭК, структурировать исходные данные для моделирования векторов кибератак с использованием базы CAPEC, поскольку данная база ориентирована на безопасность программных приложений и описывает используемые злоумышленником методы для эксплуатации известных слабых мест программного и аппаратного обеспечения. Кроме того, целесообразно формализовывать векторы атак в виде графов атак, содержащих все возможные сценарии реализации рассматриваемой кибератаки, что позволяет наглядно оценить наиболее опасные сценарии ее реализации.

Вместе с тем, использование графов атак [12-14] в их традиционном варианте затруднено неполнотой и неопределенностью исходных данных, сложностью построения и анализа графов атак без возможности их укрупнения (т.е. композиции действий злоумышленника), а также отсутствием функциональных программных решений. Ключевой проблемой построения графов атак является сложность масштабирования подхода для сети с большим количеством хостов и уязвимостей.

2. Моделирование вектора кибератак на основе композиции меташаблонов

В качестве примера промышленного объекта для моделирования вектора кибератак рассмотрим АСУ ТП транспорта товарной нефти (ТТН), интегрированную в комплексную систему оперативного контроля и управления в реальном масштабе времени, позволяющую передавать накапливаемые технологические данные о состоянии объекта в системы управления производственными процессами вышележащих уровней.

В соответствии с ГОСТ Р 62443, выделим фрагмент базовой архитектуры АСУ ТП ТТН, включающий в себя основные элементы АСУ нефтеперекачивающих станций, телекоммуникационное оборудование и линии связи (рис. 1). Наиболее опасным с точки зрения возможных последствий сценарием развития кибератаки при этом является ситуация, когда в результате несанкционированного доступа злоумышленник получает возможность управления ключевым оборудованием предприятия: становится возможным изменить транспортные потоки, спровоцировать аварии, вызвать чрезвычайные ситуации и т.д. Поэтому проанализируем угрозу перехвата управления АСУ ТП (УБИ.183 в БДУ ФСТЭК), которая заключается в возможности осуществления злоумышленником несанкционированного доступа к информационной инфраструктуре за счет получения права управления

входящей в ее состав АСУ ТП путем эксплуатации уязвимостей ее программного обеспечения или слабостей технологических протоколов передачи данных. Возможные последствия:

- остановка работы насосного оборудования нефтеперекачивающих станций;
- нарушение целостности накапливаемых данных учета принятой нефти.

Рассмотрим процесс моделирования атаки внешнего злоумышленника на АСУ ТП ТТН на основе традиционного подхода с использованием графовых моделей. При построении графа атак вначале выполняется анализ профиля вероятного злоумышленника, наиболее вероятных атак и наиболее уязвимых ресурсов предприятия. Исходя из экспертного анализа базовой модели архитектуры АСУ ТП ТТН и возможных последствий воздействия злоумышленника, рассмотрим ряд возможных сценариев (рис. 2).

Номера узлов графа соответствуют номерам устройств на рисунке 1.

$ВЗ_1$ – внешний злоумышленник, реализующий атаку на компоненты АСУ ТП.

Последствия реализации атаки:

$П_I$ – отключение насоса;

$П_{II}$ – нарушение целостности исторических данных, что ведет к искажению технико-экономических показателей системы баланса материальных потоков.

Возможные последовательности действий злоумышленника (цепочки – эксплуатация последовательности уязвимостей элементов базовой архитектуры АСУ ТП – рисунок 1) для реализации атаки (таблицы 1, 2) построены на основе экспертного анализа БДУ ФСТЭК и иных баз угроз и уязвимостей (CAPEC, CVE, NVD, CWE).

Для более подробного описания шагов злоумышленника, реализующего атаку, направленную на перехват управления АСУ ТП, и автоматизации моделирования вектора атаки, воспользуемся меташаблонами атак из CAPEC. Вектор атак представляет собой последовательность действий, совокупность способов, методов и средств, при помощи которых злоумышленник достигает поставленной цели воздействия на каждом этапе проведения атаки.

Тактики из проекта Методики, описывающие пошагово действия внешнего злоумышленника, а также соответствующие этим тактикам меташаблоны атак из CAPEC, представлены в таблице 3.

Для анализа возможностей злоумышленника на каждом этапе реализации построим граф атак для каждого меташаблона атаки, объединяющего в себе стандартные шаблоны (рис. 3-6). Стандартные шаблоны атак ориентированы на конкретную методологию или технику, используемую для осуществления атаки. Они необходимы для представления эксплуатации конкретной техники и достижения желаемой цели. Подробный шаблон атаки обеспечивает больший уровень детализации, используя конкретную технику, нацеленную на конкретную технологию.

Отметим, что построенный выше граф атак на промышленную сеть (рис. 2) опирается на исчерпывающие сведения специалистов информационной безопасности об анализируемой системе: архитектуре, внутренних ресурсах, их значимости и т.п. Внешний злоумышленник не обладает всей полнотой информации о системе и выполняет атаку на основе имеющихся у него сведений. Следовательно, для моделирования его возможных действий достаточно рассмотреть последовательность связанных меташаблонов, раскрывающих узлы 7 и 6 экспертного графа атак и соответствующих применению техник и тактик Методики. На основе графов атак меташаблонов конструируется вектор атак в виде цепочки вероятностных переходов между узлами графа атаки (рис. 7). Для оценки вероятностей переходов можно использовать соответствующие элементу меташаблона уязвимость и уровень ее опасности (оценка CVSS [15, 16]). Если конкретная уязвимость отсутствует в системе, то переход к соответствующему элементу графа меташаблона невозможен (весовой коэффициент, характеризующий вероятность перехода к следующей вершине, равен нулю).

Таблица 1

Эксплуатируемые уязвимости компонентов базовой архитектуры АСУ ТП ТТН

Компонент	Уязвимость
3	Уязвимость прикладного ПО управления версиями прошивок
6	Уязвимость ПО организации удаленного доступа в ЛВС
7	Уязвимость VPN-сервера
10	Уязвимость прикладного ПО сервера NTP
11	Уязвимость прикладного ПО SCADA клиента
12	Уязвимость прикладного ПО SCADA сервера
13	Уязвимость OPC-сервера
14	Уязвимость системного ПО сервера хранения исторических данных
16	Уязвимость коммутационного оборудования сети
20	Уязвимость механизмов авторизации ПЛК

Исходными данными для конструирования вектора атаки на основе меташаблонов являются результаты работы сканеров уязвимостей и базы данных угроз и уязвимостей, а также потенциальных слабостей программного и аппаратного обеспечения. Набор показателей системы оценки уязвимостей CVSS и базы CVE и CWE позволяют формально описать уязвимость и сценарий ее эксплуатации, а также автоматизировать процесс построения цепочки возможных переходов внутри меташаблона.

Возможны два варианта анализа графа атаки, соответствующего меташаблону:

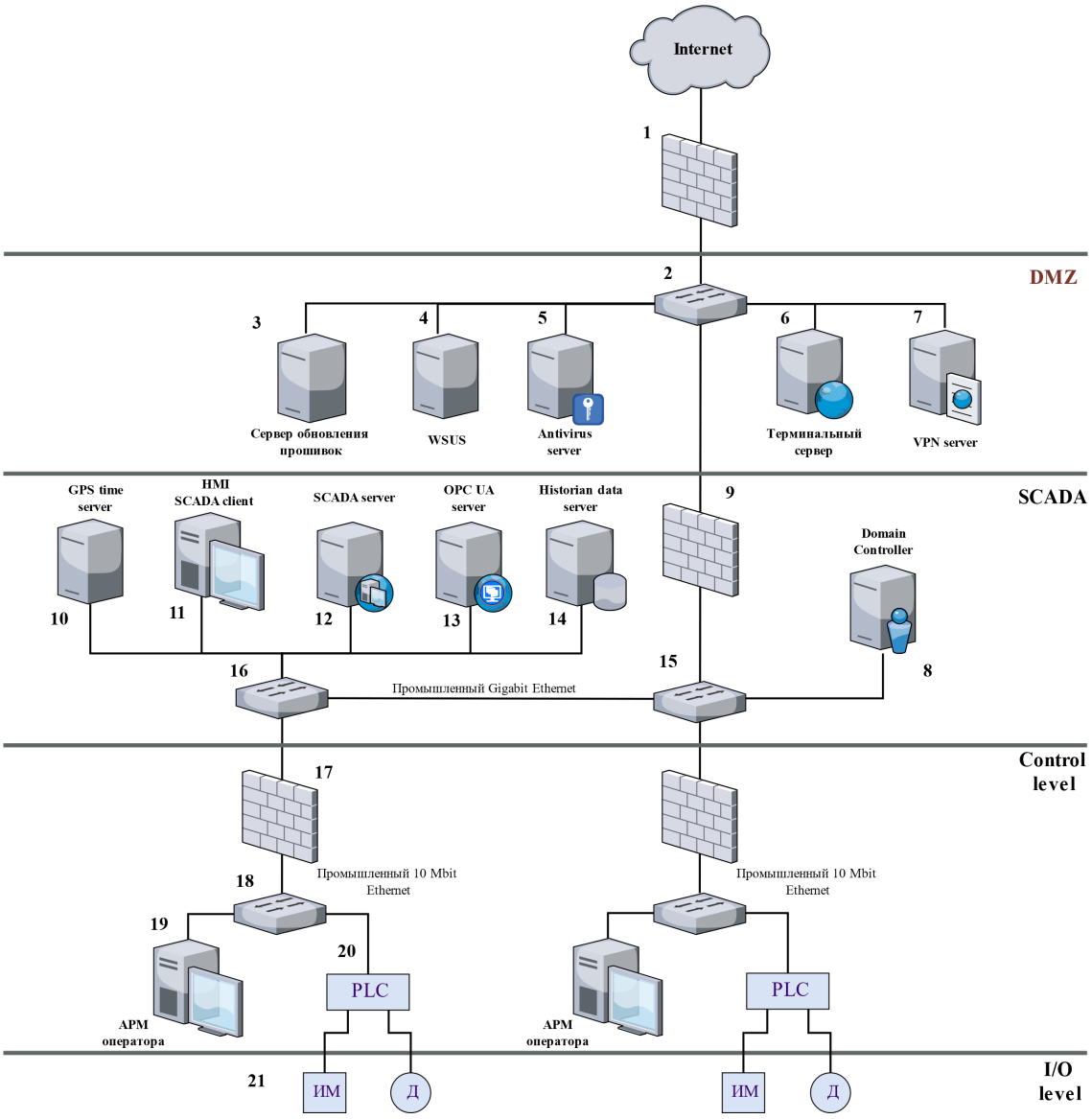


Рис.1. Базовая архитектура АСУ ТП ТТН

1) граф строится поэтапно, с моделированием по матрицам потенциальных переходов между вершинами и выбором возможных переходов при наличии уязвимостей и слабостей;

2) полный граф редуцируется – отсекаются нереализуемые переходы и вершины с нулевыми связями.

Описанный подход частично реализован в инструментах анализа защищенности информационных систем, использующих симуляцию векторов атак (Cymulate), сценарии автоматической эксплуатации уязвимостей (PenTera, Core Security, Rapid 7 Metasploit [17]), аналитическое тестирование на проникновение (CyBot). В то же время, если формируемый автоматически граф атак становится достаточно большим, это затрудняет его практический анализ экспертом.

3. Моделирование вектора кибератак в базисе нечетких когнитивных карт

Рассмотрим дальнейшую формализацию графа атак в виде иерархической нечеткой когнитивной карты, позволяющей анализировать векторы атак с требуемым уровнем детализации за счет механизмов декомпозиции и укрупнения. Процедура преобразования НКК путем ее «сворачивания» (т.е. перехода от частного к общему), и, наоборот, построения вложенной НКК путем ее «развертывания», детализации (от общего к частному) описаны в [18, 19].

В данной случае рассмотрим процедуру «сворачивания» детализированной НКК, раскрывающей содержание вектора атак, до укрупненной НКК уровня представления кибератаки. Процесс сворачивания

DOI: 10.21681/2311-3456-2021-2-2-16

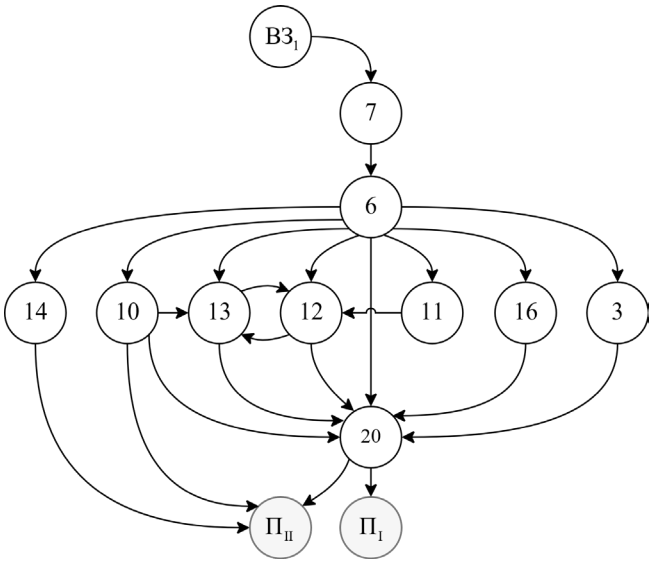


Рис.2. Граф атак на промышленную сеть АСУ ТП

Таблица 2

Последовательность действий злоумышленника для реализации атаки

Цепочка перемещений по элементам базовой архитектуры системы (рис. 1, 2)	**Результат реализации**
7 → 6 → 13 → 20	Передача команды на программируемый логический контроллер (ПЛК) для отключения насоса через OPC-сервер
7 → 6 → 12 → 20	Передача команды на ПЛК для отключения насоса через SCADA сервер
7 → 6 → 16 → 20	Подмена сетевого трафика между 11 и 12, 12 и 13, 13 и 20
7 → 6 → 14	Нарушение целостности накопленных исторических данных на сервере 14 и искажение ТЭП ТП
7 → 6 → 11 → 12 → 13	Нарушение корректной визуализации данных о ходе ТП на 11 и срабатывание защитного контура / команда оператора
7 → 6 → 10	Нарушение работы сервера NTP и нарушение целостности данных в 14
7 → 6 → 10 → 13 → 12	Задержка команд и сигналов из-за нарушения работы 10
7 → 6 → 3 → 20	Изменение работы сервера обновления прошивок ПЛК и технологического оборудования
7 → 6 → 20	Использование недостатков механизмов аутентификации и авторизации ПЛК (пароль и логин по умолчанию) для изменения режима работы ПЛК и искажения передаваемых данных

Таблица 3

Тактики и соответствующие им меташаблоны атак

Тактики / Методика	Меташаблоны атак / CAPEC
1) сбор информации о системах и сетях	1) CAPEC-169: Footprinting. Включает в себя различные методы сбора информации для подготовки к атаке. Позволяет узнать о составе, конфигурации, механизмах безопасности системы и сети (рис. 3).
2) получение первоначального доступа к компонентам систем и сетей	2) CAPEC-560: Use of Known Domain Credentials. Злоумышленник угадывает или получает законные учетные данные для аутентификации и выполнения санкционированных действий под видом аутентифицированного пользователя (рис. 4).
3)закрепление в системах и сетях	
4) повышение привилегий по доступу к компонентам систем и сетей	3) CAPEC233: Privilege Escalation. Злоумышленник использует уязвимость, позволяющую ему повысить свои привилегии и выполнить действия, которые ему не разрешено выполнять (рис. 5).
5) неправомерный доступ и воздействие на информационные ресурсы или компоненты систем и сетей, приводящее к негативным последствиям	4) CAPEC-176: Configuration / Environment Manipulation. Злоумышленник манипулирует файлами и настройками, которые влияют на поведение приложения (рис. 6).

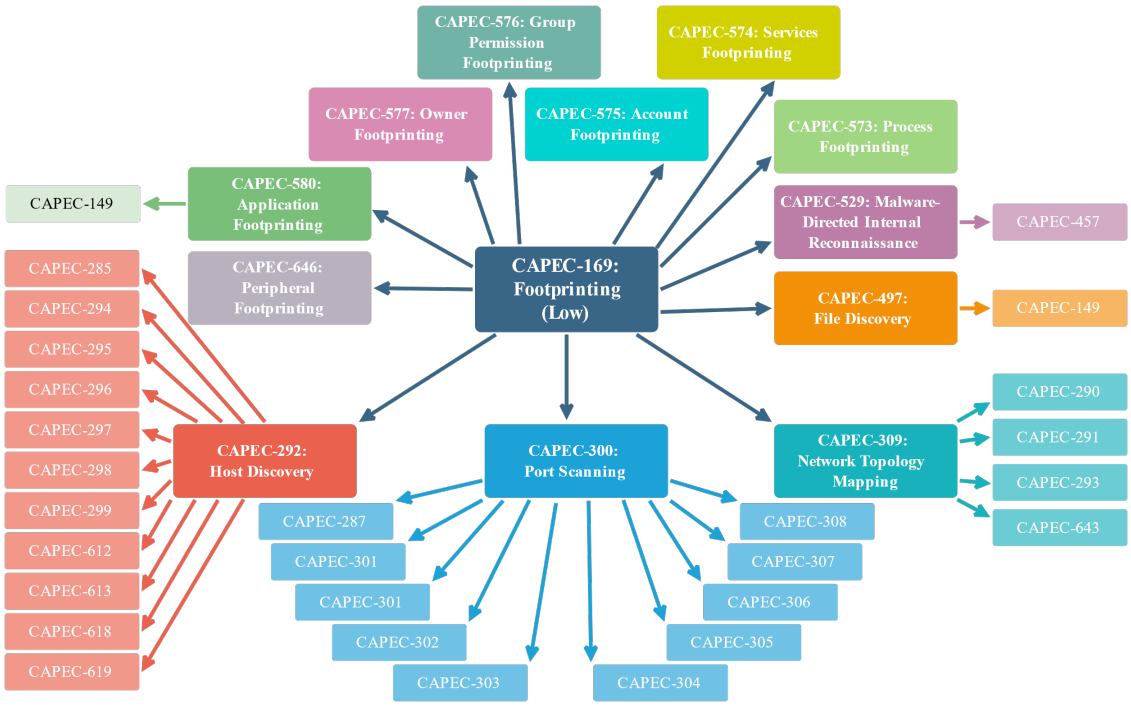


Рис.3. Граф атаки CAPEC-169: Footprinting

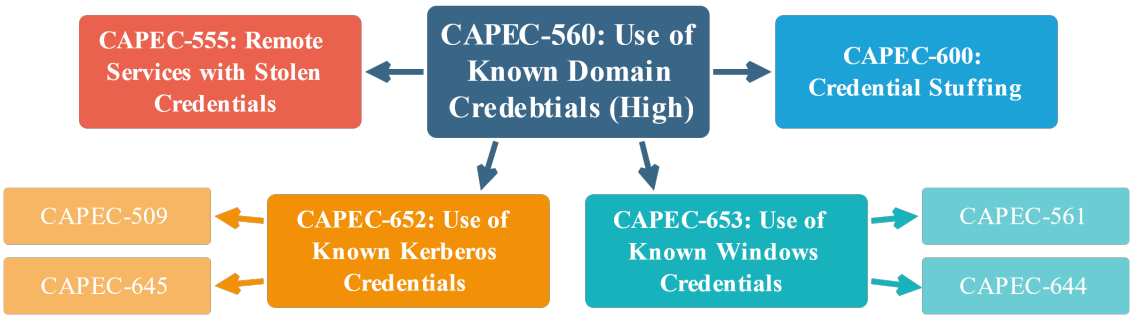


Рис.4. Граф атаки CAPEC-560: Use of Known Domain Credentials

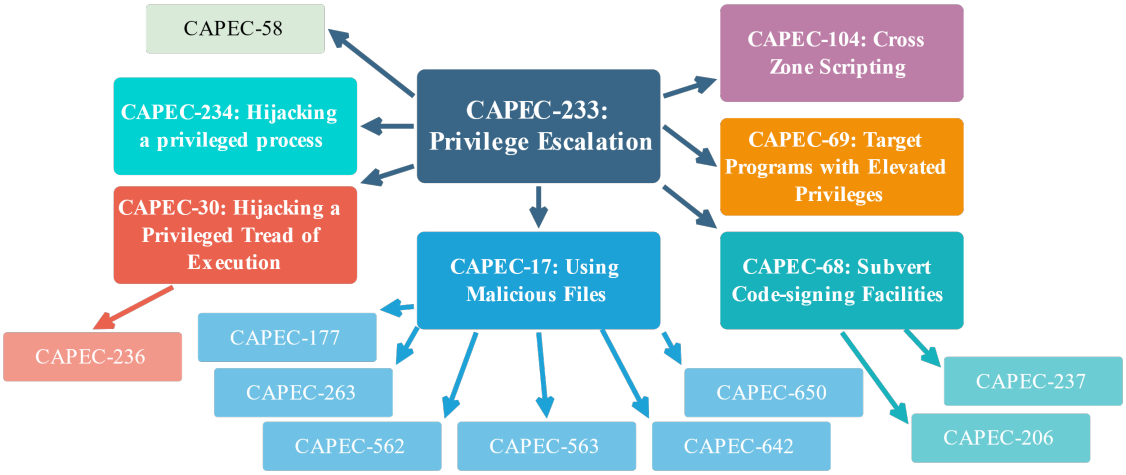


Рис.5. Граф атаки CAPEC-233: Privilege Escalation

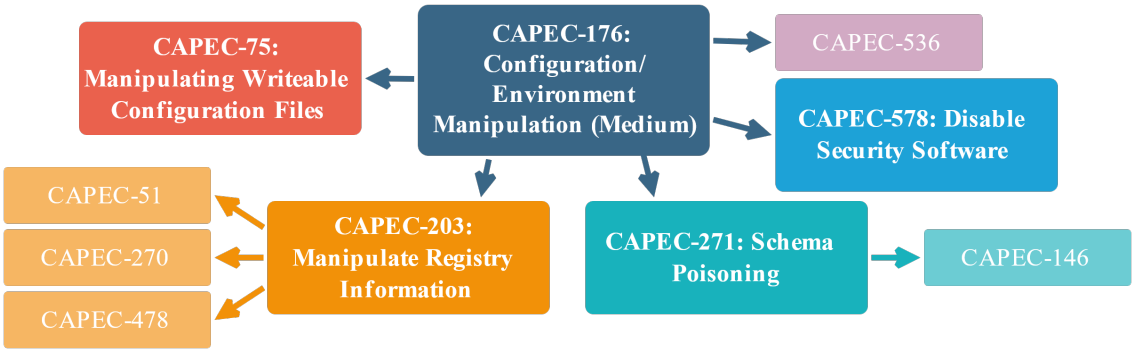


Рис.6. Граф атаки CAPEC-176: Configuration/Environment Manipulation

действий злоумышленника на хосте 7 экспертного графа атак (рис. 2) отображен на рисунке 9, где $B3_1$ – концепт-драйвер, характеризующий активного внешнего злоумышленника, а численные обозначения приведены для концептов, соответствующих элементам графа атак подробного меташаблона с привязкой к системе индексации базы шаблонов CAPEC.

Алгоритм построения укрупненной НКК для сформированного вектора атаки включает следующие шаги:

1. Композиция сценарного уровня моделирования атаки (рис. 8, I)
2. Наиболее детализированный уровень графа атаки получен на основе анализа матрицы переходов детальных меташаблонов. Вершины графа атак соответствуют концептам НКК, а веса связей – вероятностям переходов, полученным на основе оценок опасности уязвимостей CVSS.
3. Построение укрупненной НКК для представления модели атаки (рис. 8, II). Если предыдущий детализированный уровень НКК отражал ряд действий злоумышленника на каждом этапе реализации атаки, то данный уровень позволяет свернуть данные

действия до описания последовательности этапов развития атаки на основе формализованных меташаблонов, т.е. отображает сценарий реализации кибератаки.

4. Построение НКК для свернутого представления варианта отдельной атаки (рис. 8, III). Каждая атака укрупняется до концепта НКК с соответствующими весовыми коэффициентами, позволяющими оценить вероятность реализации атаки в каждом из возможных сценариев.
5. Построение НКК для моделирования набора возможных атак на выделенные целевые концепты с оценкой вероятности реализации и значимости возможных последствий (рис. 9).
6. Результирующая НКК, позволяющая оценить уровень локальных относительных рисков при реализации воздействия злоумышленника на АСУ ТП.

На рисунке 9 развернута цепочка действий злоумышленника (фрагмент Cyber Kill Chain) при реализации атаки на граничные элементы системы (хосты 7 и 1) с последующими переходами к внутренним хостам сети (3, 6 и далее – 14 и 20), достижимость которых определяется из матрицы переходов графа физической и логической топологий сети с учетом наличия уязвимостей для реализации переходов между промежуточными узлами. Целевыми концептами являются хосты 14 и 20, соответствующие серверу промежуточного хранения исторических данных и ПЛК. Соответствующими последствиями реализации атаки являются концепты $П_I$ и $П_{II}$, описанные ранее.

Множество маршрутов из начальной вершины НКК в конечную отражает множество сценариев, т.е. последовательность перемещений злоумышленника между элементами системы. Поскольку сценарий характеризуется наличием уязвимостей на всем пути злоумышленника до цели, а также метриками CVSS этих уязвимостей, то на основании НКК, моделирующей все возможные атаки на ресурсы рассматриваемой системы, формируются:

- оценка вероятности реализации атаки на внешний сервис, как первый шаг нарушителя, нацеленный на проникновении в систему предприятия;
- оценка вероятности успешного закрепления на узле;
- оценка реализации каждого этапа кибератаки в отдельности;
- оценка реализации вектора атаки на целевой ресурс, определяющая возможность реализации воздействий злоумышленника на информационную инфраструктуру предприятия для достижения целевого ресурса;
- оценка вероятности неправомерного доступа к целевому ресурсу, что говорит о успешности реализации конкретного сценария реализации кибератаки;
- оценка вероятности реализации сложной целенаправленной кибератаки;
- оценка значимости последствий, на основании которых эксперт может сделать выводы о критичности последствий реализации кибератаки.

4. Пример моделирования вектора кибератак на основе меташаблонов CAPEC с количественной оценкой риска

Серая нечеткая когнитивная карта (СНКК) – это ориентированный граф, заданный с помощью кортежа множеств [20]:

$$\text{СНКК} = \langle C, F, W \rangle,$$

где C – множество концептов, в качестве которых выступают значимые факторы (вершины графа), F – множество связей между концептами (направленные дуги) и W – множество весов связей СНКК, которые могут быть как положительными, так и отрицательными для «усиления» и «ослабления» влияния концепта соответственно.

Применение алгебры «серых» чисел при задании множества W позволяет использовать нечеткую лингвистическую шкалу с учетом степени уверенности эксперта в текущей оценке (таблица 4). Состояние концептов X также будет определяться как «серое» число.

Таблица 4

Нечеткая лингвистическая шкала для оценки силы связи между концептами (оценка взаимовлияния)

Лингвистическое значение	Диапазон	Обозначение терма
Не влияет	0	Z
Очень слабая	(0; 0,15]	VL
Слабая	(0,15; 0,35]	L
Средняя	(0,35; 0,6]	M
Сильная	(0,6; 0,85]	H
Очень сильная	(0,85; 1]	VH

Согласно предложенному алгоритму, строится НКК (рис. 10, I), соответствующая детализированному уровню графа атаки (рис. 8, I). На основе детализированной НКК с учетом оценок взаимовлияния и установившегося состояния концептов строится НКК (рис. 10, II, где A_j^i – концепт, состояние которого соответствует оценке вероятности реализации сценария атаки злоумышленника, закрепившегося на i-узле сети, на j-узел) для свернутого представления варианта отдельной атаки внешнего злоумышленника на VPN-сервер базовой архитектуры сети (хост 7).

Следующим шагом является построение НКК (рис. 11) для моделирования набора возможных атак на выделенные целевые концепты базовой архитектуры с оценкой вероятности реализации и значимости возможных последствий.

$C_{ВЗ_1}$ – внешний злоумышленник, реализующий атаку на компоненты АСУ ТП; $C_{П_I}$ – остановка работы насосного оборудования; $C_{П_{II}}$ – нарушение целостности исторических данных.

DOI: 10.21681/2311-3456-2021-2-2-16

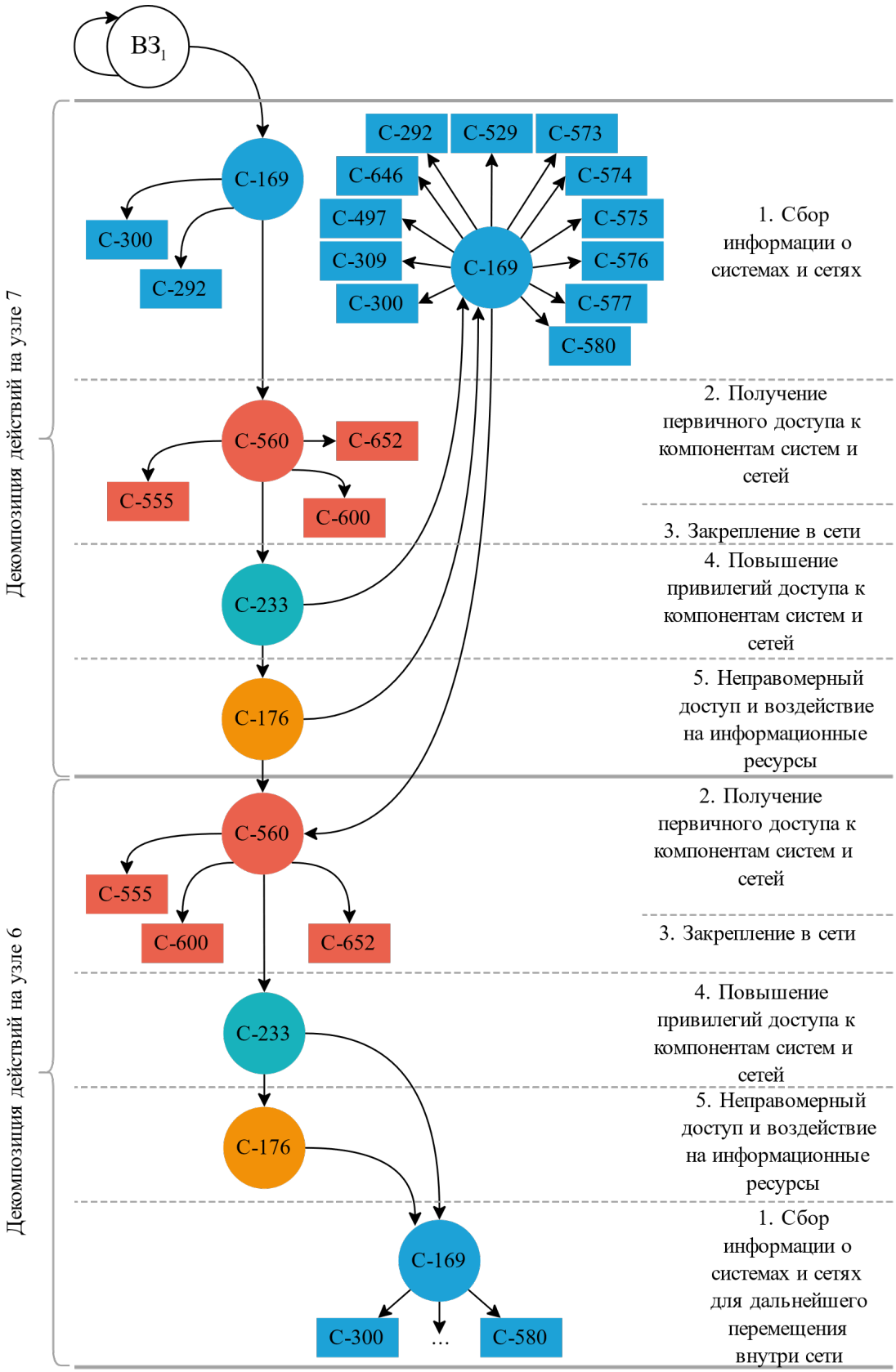


Рис.7. Применение сценарного подхода к моделированию сложной атаки на основе шаблонов атак CAPEC для фрагмента графа атак

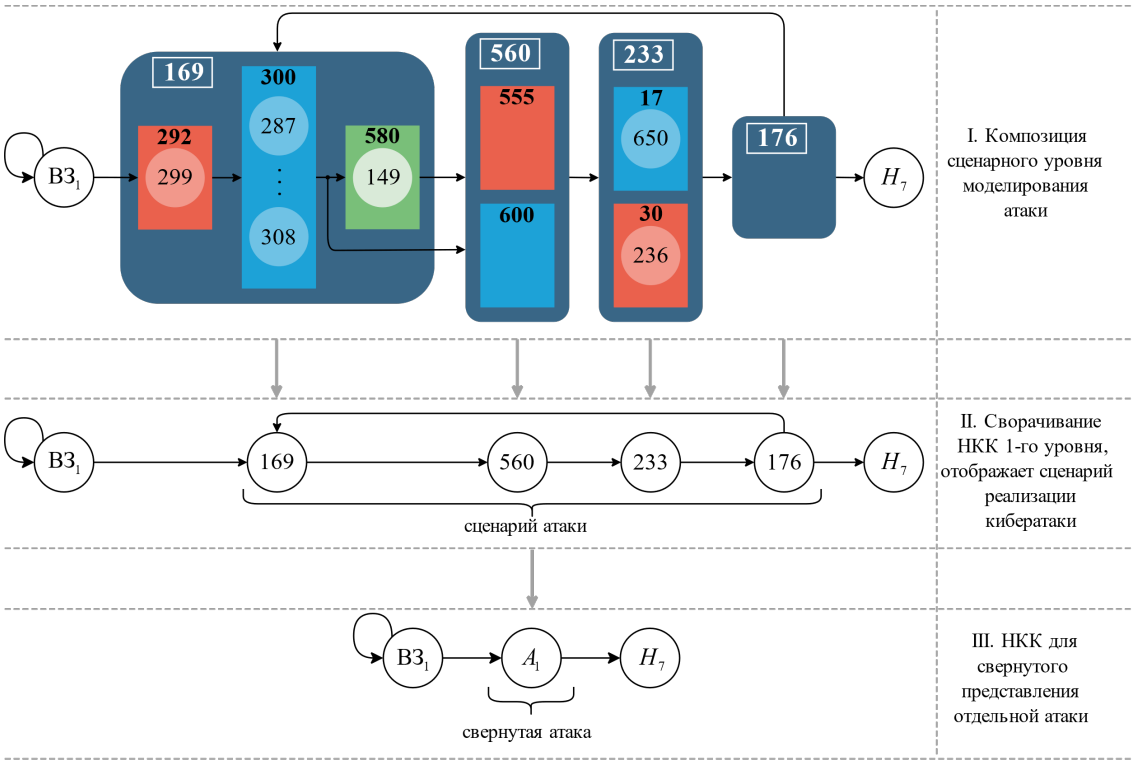


Рис.8. Этапы построения укрупненной НКК для формализации детального графа атаки

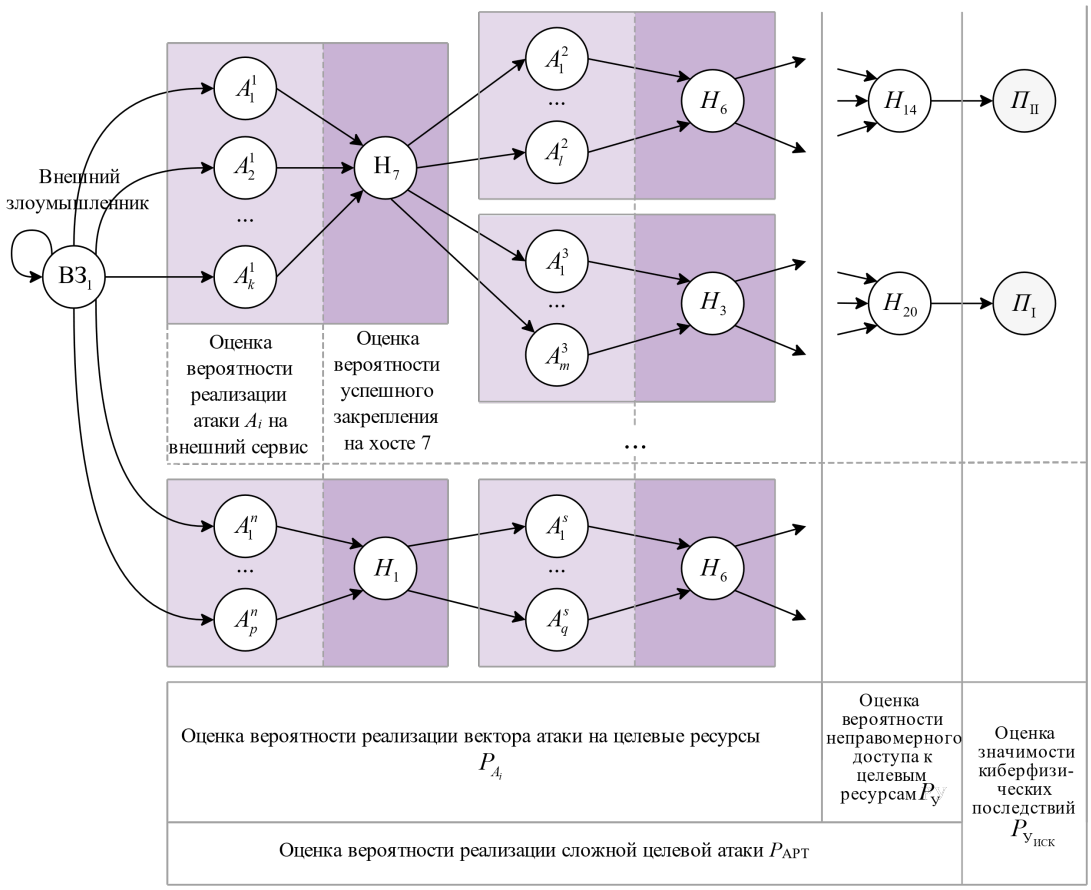


Рис.9. НКК для моделирования набора возможных атак на выделенные целевые концепты

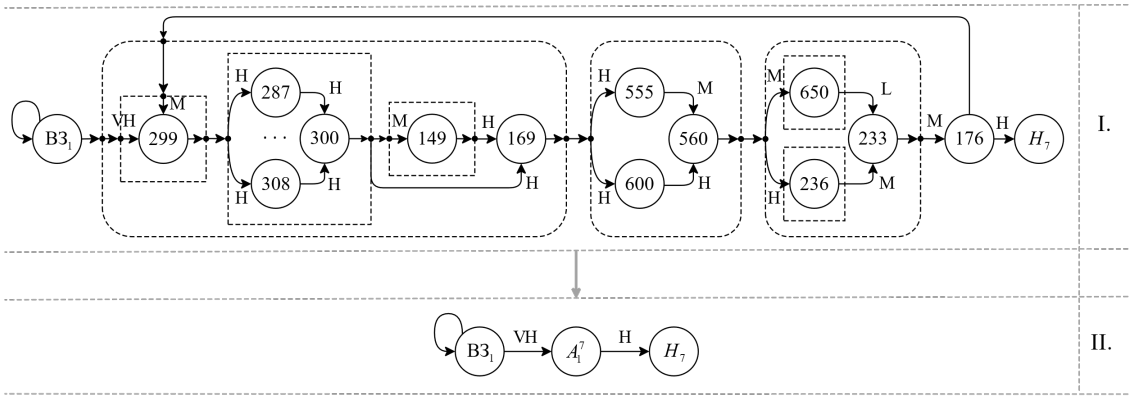


Рис.10. НКК, моделирующая атаку на хост 7

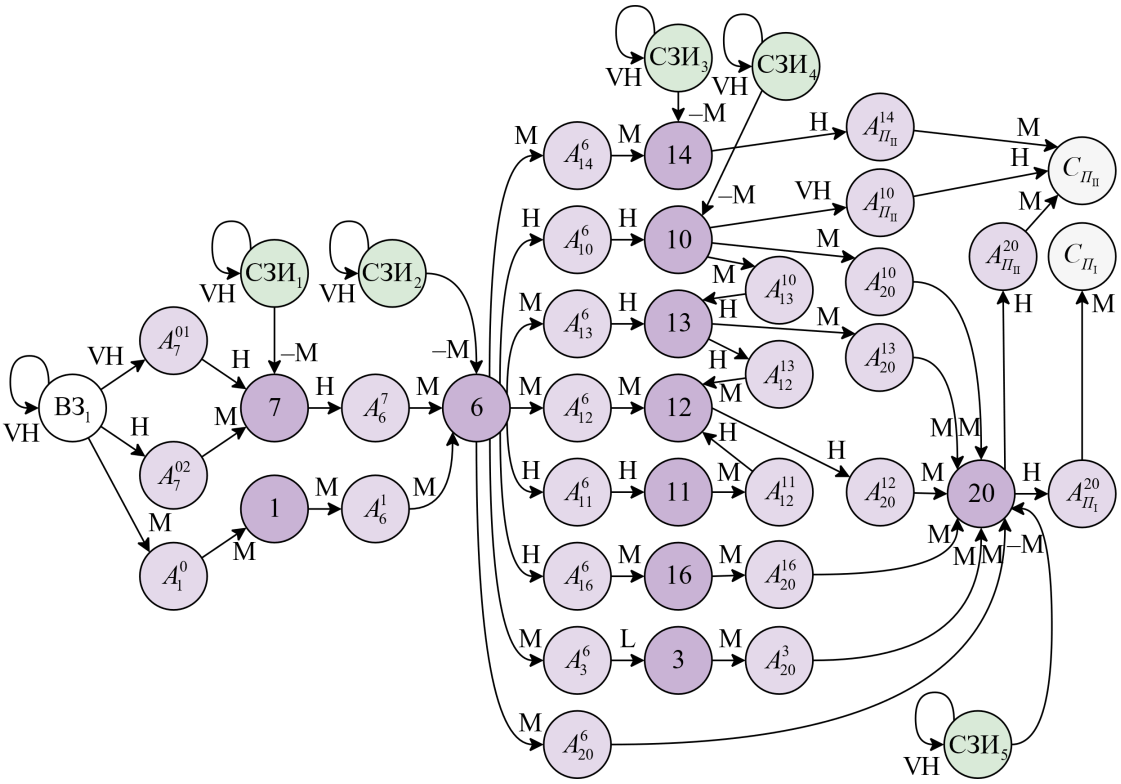
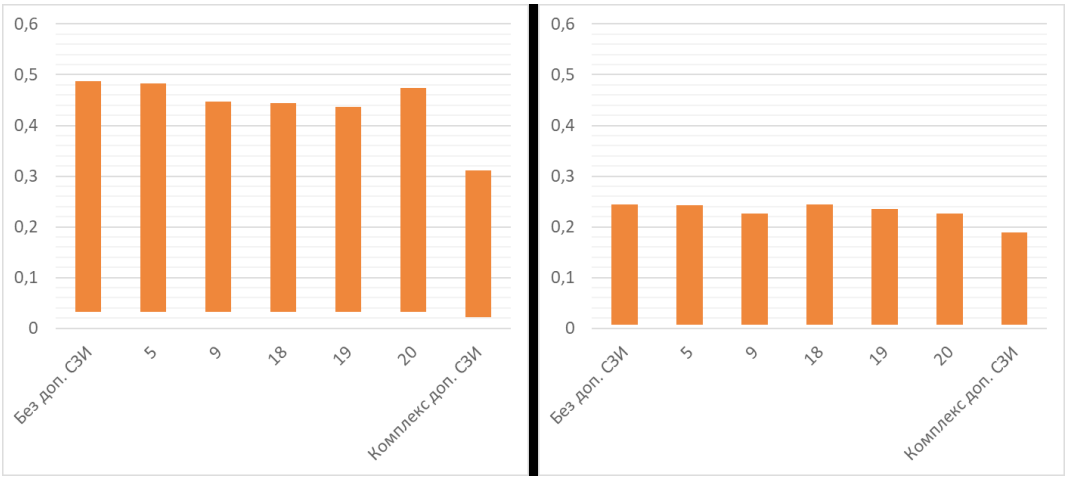


Рис.11. НКК, моделирующая возможные атаки на выделенные целевые концепты базовой архитектуры

С учетом определенных на предыдущем шаге установившихся значений концептов A_j^i рассчитываются оценки локальных относительных рисков остановки работы насосного оборудования ($C_{П_I}$) и нарушения целостности исторических данных ($C_{П_{II}}$) (таблица 5). При анализе максимального потока в ориентированном графе НКК из вершины $ВЗ_1$ в целевые вершины $C_{П_I}$ и $C_{П_{II}}$) с помощью алгоритма Форда-Фалкерсона можно выделить [21] наиболее критичные узлы сети (C_9, C_{18}, C_{19}, C_5, C_{20}), закрепление на которых позволяет злоумышленнику реализовать атаки, приводящие к наиболее значительным последствиям. Следовательно, для выделенных узлов рассмотрим применение соответствующих дополнительных средств защиты информации (концепты $C_{СЗИ_2}$, $C_{СЗИ_3}$, $C_{СЗИ_4}$, $C_{СЗИ_5}$). Интервальные значения соответствующих целевых концептов $C_{П_I}$ (рис. 12, а) и $C_{П_{II}}$ (рис. 12, б) при реализации каждого из сценариев позволяют оценить эффективность применяемых СЗИ.

Показатели локального относительного риска для ключевых ресурсов снизились в среднем на 15-20 %, что свидетельствует об эффективности рекомендуемых мер нейтрализации кибератак.



а) б)

Рис.12. Интервальные значения целевых концептов $C_{П_I}$(а) и $C_{П_{II}}$(б) при моделировании сценариев реализации сложной атаки внешнего злоумышленника на целевые ресурсы: без дополнительных СЗИ, дополнительные СЗИ применяются для ключевых узлов базовой архитектуры сети (C_5, C_9, C_{18}, C_{19}, C_{20}), применяется комплекс доп. СЗИ

Таблица 5

Оценка локальных относительных рисков

Сценарий	Остановка работы насосного оборудования ($C_{П_I}$)	Нарушение целостности исторических данных ($C_{П_{II}}$)
Без применения дополнительных СЗИ	[0,0073; 0,2366]	[0,0323; 0,4544]
СЗИ для узла C_5	[0,0073; 0,2352]	[0,0323; 0,4511]
СЗИ для узла C_9	[0,0072; 0,2192]	[0,0322; 0,4545]
СЗИ для узла C_{18}	[0,0073; 0,2366]	[0,0317; 0,4120]
СЗИ для узла C_{19}	[0,0072; 0,2286]	[0,0322; 0,4045]
СЗИ для узла C_{20}	[0,0073; 0,2189]	[0,0323; 0,4414]
Применение комплекса СЗИ для узлов C_5, C_9, C_{18}, C_{19}, C_{20}	[0,0071; 0,1818]	[0,0223; 0,2883]

Заключение

Автоматизированное моделирование набора возможных атак на компоненты базовой архитектуры АСУ ТП ТТН позволяет извлечь информацию о слабых местах инфраструктуры, наиболее опасных уязвимостях и потенциальных слабостях компонент системы, выявить наиболее успешные сценарии реализации атак и оценить их последствия для предприятия. Исходными данными для построения когнитивных карт становятся не только экспертные оценки (граф атак), но и формализованные и систематизированные шаблоны из международных баз знаний, что существенно повышает обоснованность и полноту сценарного моделирования. Применение данного подхода позволит получить подробную оценку рисков кибербезопасности и, как следствие, обеспечить более обоснованный выбор средств для реализации стратегии многоуровневой эшелонированной защиты (Defense in depth).

Традиционно используется построение вектора в виде графа атак, однако пошаговое описание реализации кибератаки на АСУ ТП вызывает трудности с масштабируемостью графа атак и затруднения у экспертов в процессе его практического анализа. Кроме того, неполнота и противоречивость исходных данных затрудняет оценку вероятностных переходов при анализе вектора атак. Построение НКК для моделирования набора всех возможных атак и их сценариев реализации облегчает специалистам анализ защищенности и позволяет на этапе архитектурного проектирования информационной системы заложить

DOI: 10.21681/2311-3456-2021-2-2-16

основные средства и инструменты защиты. В результате анализа вектора кибератак эксперт может определить все возможные сценарии реализации с учетом используемых уязвимостей, оценить уровень опасности реализации каждого сценария в отдельности и кибератаки в целом.

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта № 1/2020 (моделирование НКК) и при финансовой поддержке РФФИ в рамках научного проекта № 20-38-90078 (декомпозиция меташаблонов).

Литература

1. El Hariri M. et al. A targeted attack for enhancing resiliency of intelligent intrusion detection modules in energy cyber physical systems. In 19th International Conference on Intelligent System Application to Power Systems (ISAP). IEEE, 2017, pp. 1-6.
2. Alshamrani A. et al. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities // IEEE Communications Surveys & Tutorials. 2019. № 2 (21). С. 1851-1877.
3. Yadav T., Rao A.M. Technical aspects of cyber kill chain // International Symposium on Security in Computing and Communication. Springer, Cham. 2015. Pp. 438-452.
4. Khan M.S., Siddiqui S., Ferens K. A cognitive and concurrent cyber kill chain model // Computer and Network Security Essentials. Springer, Cham. 2018. С. 585-602.
5. Мельников П.В., Ешенко Р.А. Проблемы формирования модели угроз информационной безопасности в информационных системах // Вестник науки. 2020. № 1 (6). С. 185-189.
6. Strom B.E. et al. Finding cyber threats with ATT&CK-based analytics // The MITRE Corporation, Bedford, MA, Technical Report № MTR170202. 2017. 38 p.
7. Al-Shaer R., Ahmed M., Al-Shaer E. Statistical Learning of APT TTP Chains from MITRE ATT&CK. In Proc. RSA Conf. 2018. Pp. 1-2.
8. Munaiah N. et al. Characterizing Attacker Behavior in a Cybersecurity Penetration Testing Competition. In 2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM). IEEE, 2019, pp. 1-6.
9. Kotenko I., Doynikova E. The CAPEC based generator of attack scenarios for network security evaluation. In 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). IEEE, 2015, № 1, pp. 436-441.
10. Brazhuk A. Semantic model of attacks and vulnerabilities based on CAPEC and CWE dictionaries // International Journal of Open Information Technologies. 2019. № 3 (7). С. 38-41.
11. Noel S. Interactive visualization and text mining for the CAPEC cyber-attack catalog. In Proceedings of the ACM Intelligent User Interfaces Workshop on Visual Text Analytics. 2015.
12. Zhang Y. et al. Power system reliability evaluation with SCADA cybersecurity considerations // IEEE Transactions on Smart Grid. 2015. № 4 (6). Pp. 1707-1721.
13. Дойникова Е.В., Котенко И.В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер // Информационная безопасность. 2018. № 2 (57). С. 211-240.
14. Mell P., Harang R. Minimizing Attack Graph Data Structures. In the Tenth International Conference on Software Engineering Advances (Barcelona, Spain), 2015, pp. 376-385.
15. Doynikova E., Kotenko I. CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection. In 2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP). IEEE, 2017, pp. 346-353.
16. Doynikova E.V., Fedorchenko A.V., Kotenko I.V. Detection of Weaknesses in Information Systems for Automatic Selection of Security Actions // Automatic Control and Computer Sciences. 2019. № 8 (53). Pp. 1029-1037.
17. Bullock J., Parker J.T. Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework // John Wiley & Sons, 2017.
18. Harmati I.A., Koczy L.T. On the Convergence of Fuzzy Grey Cognitive Maps // Information Technology, Systems Research, and Computational Physics. Springer Verlag. 2018. Pp. 74-84.
19. Wu K. et al. Online Fuzzy Cognitive Map Learning // IEEE Transactions on Fuzzy Systems. 2020. P. 1
20. Васильев В.И., Вульфин А.М., Гузаиров М.Б., Картак В.М., Черняховская Л.Р. Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт // Информационные технологии. 2020. № 4 (26). С. 213-221.
21. Васильев В.И., Вульфин А.М., Черняховская Л.Р. Анализ рисков инновационных проектов с использованием технологии многослойных нечетких когнитивных карт // Программная инженерия. 2020. № 3 (11). С. 142-151.

COGNITIVE MODELING OF THE CYBER ATTACK VECTOR BASED ON CAPEC METHODS

Vasilyev V.I.[5], Kirillova A.D.[6], Vulfin A.M.[7]

Purpose: *automation of complex attack vector modeling based on formalized CAPEC meta-pattern based on fuzzy cognitive maps.*

Methods: *modeling a tool in the form of a graph with a further form of development in the form of a hierarchical fuzzy cognitive map for analysis using the potential level of detail and quantitative assessment of cybersecurity risks.*

Practical relevance: *a scenario approach to modeling complex multistep targeted cyberattacks is proposed based on the draft Methodology for modeling security threats of the FSTEC of Russia and the base of meta- pattern for attacks CAPEC. The algorithm for "folding" a detailed fuzzy cognitive map of the attack vector is shown using the example of the threat of interception of control of an automated process control system of an oil company with an assessment of the probability of implementation, considering the severity level of exploited vulnerabilities. The main software modules of the system have been developed. Computational experiments were carried out to assess the effectiveness of its application. It is shown that as a result of analyzing the vector of cyberattacks in a fuzzy cognitive basis, an expert can rank possible scenarios of implementation, considering the vulnerabilities used, assess the level of danger of the implementation of each scenario separately and cyberattacks as a whole.*

Keywords: *fuzzy cognitive map, risk assessment, attack graph, scenario, attack pattern, vulnerabilities, Defense in depth*

References

1. El Hariri M. et al. A targeted attack for enhancing resiliency of intelligent intrusion detection modules in energy cyber physical systems. In 19th International Conference on Intelligent System Application to Power Systems (ISAP). IEEE, 2017, pp. 1-6.
2. Alshamrani A. et al. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities // IEEE Communications Surveys & Tutorials, 2019, No 2 (21), pp. 1851-1877.
3. Yadav T., Rao A.M. Technical aspects of cyber kill chain // International Symposium on Security in Computing and Communication, Springer, Cham, 2015, pp. 438-452.
4. Khan M.S., Siddiqui S., Ferens K. A cognitive and concurrent cyber kill chain model // Computer and Network Security Essentials, Springer, Cham, 2018, pp. 585-602.
5. Melnikov P.V., Eshenko R.A. Problemy formirovanija modeli ugroz informacionnoj bezopasnosti v informacionnyh sistemah // Vestnik nauki, 2020, No 1 (6), pp. 185-189.
6. Strom B.E. et al. Finding cyber threats with ATT&CK-based analytics // The MITRE Corporation, Bedford, MA, Technical Report № MTR170202, 2017.
7. Al-Shaer R., Ahmed M., Al-Shaer E. Statistical Learning of APT TTP Chains from MITRE ATT&CK. In Proc. RSA Conf., 2018, pp. 1-2.
8. Munaiah N. et al. Characterizing Attacker Behavior in a Cybersecurity Penetration Testing Competition. In 2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM). IEEE, 2019, pp. 1-6.
9. Kotenko I., Doynikova E. The CAPEC based generator of attack scenarios for network security evaluation. In 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). IEEE, 2015, No 1, pp. 436-441.
10. Brazhuk A. Semantic model of attacks and vulnerabilities based on CAPEC and CWE dictionaries // International Journal of Open Information Technologies, 2019, No 3 (7), pp. 38-41.
11. Noel S. Interactive visualization and text mining for the CAPEC cyber attack catalog. In Proceedings of the ACM Intelligent User Interfaces Workshop on Visual Text Analytics, 2015.
12. Zhang Y. et al. Power system reliability evaluation with SCADA cybersecurity considerations // IEEE Transactions on Smart Grid, 2015, No 4 (6), pp. 1707-1721.

5 Vladimir Vasilyev, Dr.Sc. (Eng.), Professor, Professor of Department of Computer Engineering and Information Security, Ufa State Aviation Technical University, Ufa, Russia. E-mail: vasilyev@ugatu.ac.ru.

6 Anastasia Kirillova, postgraduate of Department of Computer Engineering and Information Security, Ufa State Aviation Technical University, Ufa, Russia. E-mail: kirillova.andm@gmail.com

7 Alexey Vulfin, Ph.D., Associate Professor of Department of Computer Engineering and Information Security, Ufa State Aviation Technical University, Ufa, Russia. E-mail: vulfin.alexey@gmail.com

DOI: 10.21681/2311-3456-2021-2-2-16

13. Dojnikova E.V., Kotenko I.V. Sovershenstvovanie grafov atak dlja monitoringa kiberbezopasnosti: operirovanie netochnostjami, obrabotka ciklov, otobrazhenie incidentov i avtomaticheskij vybor zashhitnyh mer // Informacionnaja bezopasnost', 2018, No 2 (57), pp. 211-240.
14. Mell P., Harang R. Minimizing Attack Graph Data Structures. In the Tenth International Conference on Software Engineering Advances (Barcelona, Spain), 2015, pp. 376-385.
15. Doynikova E., Kotenko I. CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection. In 2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), IEEE, 2017, pp. 346-353.
16. Doynikova E.V., Fedorchenko A.V., Kotenko I.V. Detection of Weaknesses in Information Systems for Automatic Selection of Security Actions // Automatic Control and Computer Sciences, 2019, No 8 (53), pp. 1029-1037.
17. Bullock J., Parker J.T. Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework // John Wiley & Sons, 2017.
18. Harmati I.A., Koczy L.T. On the Convergence of Fuzzy Grey Cognitive Maps // Information Technology, Systems Research, and Computational Physics, Springer Verlag, 2018, pp. 74-84.
19. Wu K. et al. Online Fuzzy Cognitive Map Learning // IEEE Transactions on Fuzzy Systems. 2020. С. 1
20. Vasilyev V.I., Vulfin A.M., Guzairov M.B., Kartak V.M., Chernjahovskaja L.R. Ocenka riskov kiberbezopasnosti ASU TP promyshlennyh ob#ektov na osnove vlozhennyh nechetkih kognitivnyh kart // Informacionnye tehnologii, 2020, No 4 (26), pp. 213-221.
21. Vasilyev V.I., Vulfin A.M., Chernjahovskaja L.R. Analiz riskov innovacionnyh proektov s ispol'zovaniem tehnologii mnogoslojnyh nechetkih kognitivnyh kart // Programmnaja inzhenerija, 2020, No 3 (11), pp. 142-151.