DOI: 10.55648/1998-6920-2023-17-4-49-61 УДК 04.056.5:378.3

Формирование вектора сетевых атак с учетом специфики связей техник и тактик

И. А. Ветров[1], В. В. Подтопельный[2]

[1] Балтийский федеральный университет им. И. Канта
[2] Калининградский государственный технический университет

Аннотация: Рассмотрены проблемы, возникающие при решении задачи построения вектора атаки в сетевой инфраструктуре. Приведены и охарактеризованы разновидности различных тактик и техник методик ФСТЭК, применяемых при построении вектора сетевой атаки, а также рассмотрена специфика их взаимосвязей с использованием марковских цепей при моделировании атакующих воздействий, рассмотрена их пригодность для различных процедур определения параметров вектора. При построении вектора сетевой атаки приводятся особенности определения вероятностей переходов системы в различные состояния компрометации сети. Формирование вектора атаки изучается в контексте эксплуатации многоуровневой корпоративной информационной системы. Определяются особенности построения упрощенного вектора атаки с учетом специфики связей тактик (состояний).

Ключевые слова: вектор атаки, информационная система, корпоративная сеть, уязвимость, марковские процессы, злоумышленник, тактики.

Для цитирования: Ветров И. А., Подтопельный В. В. Формирование вектора сетевых атак с учетом специфики связей техник и тактик // Вестник СибГУТИ. 2023. Т. 17, № 4. С. 49–61. https://doi.org/10.55648/1998-6920-2023-17-4-49-61.

Статья поступила в редакцию 25.05.2023;
принята к публикации 07.06.2023.

1. Введение

В государственных учреждениях Российской Федерации для формирования вектора атаки, создаваемого в процессе аудита, используются различные руководящие документы государственных регуляторов в области информационной безопасности. Одним из основных документов является «Методика оценки угроз безопасности информации» ФСТЭК (далее – Методика). Описанный в данном документе способ построения вектора атаки предлагает использование тактик и принадлежащих им техник (различные приемы достижения некоего результирующего состояния, интерпретируются как тактика). При описании действий злоумышленника применяются разнообразные массивы данных о признаках угроз и уязвимостях. Затем с учетом экспертного мнения формируются векторы атак. При этом допускаются заимствования различных, в том числе зарубежных, способов описания сценариев реализации угрозы (CAPEC, OWASP, STIX, WASC, ATT&CK и др.) [1]. Также при формировании вектора учитывается потенциал возможных нарушителей (уровень их квалификации, средства атаки, цели).

Приведённая методика ориентирована на анализ открытых и распределенных информационных систем, использующих клиентско-серверную организацию, при этом не исключается рассмотрение локальных (замкнутых) систем. Однако в самой методике хотя и рассматривается понятие вероятности реализации различных тактик (фактически подразумевается прогноз возможных действий злоумышленника), сами численные значения вероятностей не применяются при описании сценария атаки. При этом описание вероятностей сопряжения и применения тактик основываются на экспертной оценке.

Таким образом, предлагаемое в методике описание сценария реализации несанкционированного доступа и вредоносного воздействия не подразумевает формальный учёт вероятностных показателей реализуемых тактик и, соответственно, техник злоумышленника, что не позволяет отследить изменение состояния вектора атаки при его развертывании.

Сегодня аспекты формирования сценария атаки исследуются разными способами. В частности, формирование векторов атаки изучают в контексте описания моделей угроз безопасности многоуровневых систем критически важных объектов. При составлении моделей могут использоваться табличные методы оценки риска [3]. Другие исследователи акцентируют свое внимание на методиках статистического анализа. В частности, предполагается «выявление аномалий в сетевом трафике за счет определения степени самоподобия трафика с использованием фрактального анализа и статистических методов» [4]. Также разрабатываются методики, учитывающие выявление взаимного влияния отдельных компьютерных атак на средства защиты сети [5]. Применяются различные методы искусственного интеллекта (нейронные сети, генетические алгоритмы, модели фильтрации на основе машинного обучения), вероятностные методы. В частности, используются различные виды марковских сетей. Предлагается использовать марковские и полумарковские модели описания действий злоумышленника для вычисления основных стационарных характеристик процесса проведения атаки [6]. Также описываются с помощью марковских процессов сценарии атак, модели функционирования сети с распределенными атакующими элементами [7]. Рассмотренные методики описания атак не связаны напрямую со специфическими особенностями способа формирования вектора атаки Методики ФСТЭК.

Таким образом, для более точного определения специфики атакующих воздействий предложенный в Методике способ построения вектора атаки можно дополнить простыми (то есть не вызывающими затруднения при построении модели угроз и в целом при аудите информационной безопасности) формальными способами определения вероятностей реализации тактик в едином сценарии с учетом вероятностей сопряжения различных техник, приводимых в Методике. Построение модели атаки с учетом вероятностей переходов из одного состояния компрометации в другое позволит прогнозировать появление событий безопасности в информационной системе с учетом атакующих воздействий внешнего нарушителя [2].

2. Проблемная область формирования вектора атаки

В большинстве случаев при аудите инфраструктуры организации изучается состояние безопасности многосегментной корпоративной информационной системы (КИС). Атакуемая сеть распределенного типа рассматривается как единое целое [7]. При атаке проявляются маркеры событий безопасности. Совокупность подобных маркеров интерпретируется как состояние из набора тактик, достигаемое техниками из приведенного в Методике списка (само осуществление техники уже может интерпретироваться как некое состояние компрометации). Сопряжение данных состояний, распределённых по времени и последовательно проявляющихся, требуется ассоциировать с компонентами инфраструктуры предприятия. Таким образом, формируется модель связанных между собой этапов атаки с учетом сетевой топологии.

При этом следует учитывать специфику модели нарушителя (в данном случае рассматривается внешний нарушитель). Соответственно, последовательность атакующих воздействий будет начинаться за границами описываемого сегмента сети, если атака реализуется по

отношению к сегменту, или за границами сети (при атаке на сеть в целом). Следует учитывать, что состояние компрометации сегмента сети может быть следствием компрометации всей инфраструктуры, которая была заражена после успешной атаки на другой ее сегмент. Поэтому необходимо четкое понимание того, где проходят границы сети и границы ее сегментов. При описании сценария компрометации всей инфраструктуры организации вектор атаки одного сегмента будет лишь одним из множества векторов и, следовательно, будет обозначен как один из множества этапов атакующих воздействий. Соответственно, вектор будет включен в общий граф состояний компрометации всей сети как одна из его вершин [6].

Нужно сказать, что при подобном подходе, следуя Методике оценки угроз ФСТЭК, критерием успешности атаки будет считаться не минимизация времени действий нарушителя (предполагается, что при более длительном проведении атаки злоумышленник рискует быть обнаруженным, и, следовательно, атака будет прервана), а сам факт достижения состояния реализации тактики № 10 («Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям») [1]. В таком случае следует определить причинно-следственные связи, которые позволили реализоваться конечному состоянию, маркирующему успешность атакующих действий. Соответственно, требуется исследовать промежуточные состояния между начальными техниками и конечными, их взаимосвязи, рассмотреть их возможные переходы из одного состояния в другое для достижения конечного состояния.

Также следует понимать, что событие, которое распознаётся как признак реализации одной из техник, может фиксироваться не только на начальных этапах компрометации, но и на промежуточных этапах (состояниях) развёртываемой атаки [7]. Задача аналитика безопасности состоит в том, чтобы определить специфику этого события, то есть его класс в соответствии с предложенной в Методике классификацией. Это необходимо для выявления либо предшествующий последовательности действий злоумышленника, которые были не замечены системами безопасности и которые следует обнаружить, либо последующей последовательности [8]. Воздействие на ресурсы инфраструктуры предприятия может произойти в любой момент, поэтому процесс перехода из состояния работоспособности в состояние аномального характера можно представить в виде дискретной марковской последовательности.

Таким образом, используя принципы формирования марковских цепей, можно создать вектор атаки с учетом вероятностей реализации разных этапов (состояний) компрометации и далее определить модель атаки.

3. Построение вектора атаки с учетом тактик атакующих воздействий

При построении вектора атаки создается последовательность связанных состояний, которые реализуются в виде череды фиксируемых в определённый период времени событий, маркирующих состояние компрометации на сетевых узлах. Последовательность состояний (маркируемых событий) с учетом периода фиксации и очередности событий, классифицируемых по принадлежности к тактикам, формируется с учетом возможного наличия других векторов атак. При этом в каждом случае предполагается различная величина вероятностей переходов к новым состояниям, которые ориентированы на приближение к итоговым целям злоумышленника. Это позволяет определить не только возможность реализации атаки в целом, но и отнести к какой-либо вероятностной последовательности некое маркированное событие безопасности, то есть к ряду событий конкретной атаки в череде множества атак [9]. В итоге это влияет на приоритет ветви вектора при выборе сценария действий злоумышленника, а значит, позволяет определить актуальность вектора. Таким образом, основным параметром в описании вектора состояний является вероятность перехода некоего компрометированного состояния в новое в соответствии с последовательностью классифицируемых в Методике тактик. На основе параметров вероятностей переходов и начальных состояний можно сформировать граф. Для этого необходимо ассоциировать тактики и состояния, которые будут

являться вершинами графа, описывающего марковские процессы. По требованиям Методики предполагается их последовательное соединение.

Выделяются следующие типы состояний, являющиеся результатом осуществления тактик:

1. Разведка (поиск и агрегация информации о системах и сетях целевой инфраструктуры) (Т1).
2. Первичная компрометация инфраструктурных компонентов систем и сетей (Т2).
3. Внедрение и эксплуатация средств разрушающего программного воздействия в системах и сетях (Т3).
4. Получение прав пользователя и сохранение доступа к системе или сети (Т4).
5. Управление средствами разрушающего программного воздействия в системах, сетях и (или) скомпрометированными компонентами (Т5).
6. Повышение уровня доступа к компонентам систем и сетей (Т6).
7. Сокрытие действий и применяемых при атаке средств (Т7).
8. Компрометация смежных подсистем (Т8).
9. Поиск и вывод данных из системы (Т9).
10. Несанкционированный доступ и компрометация инфраструктуры (Т10).

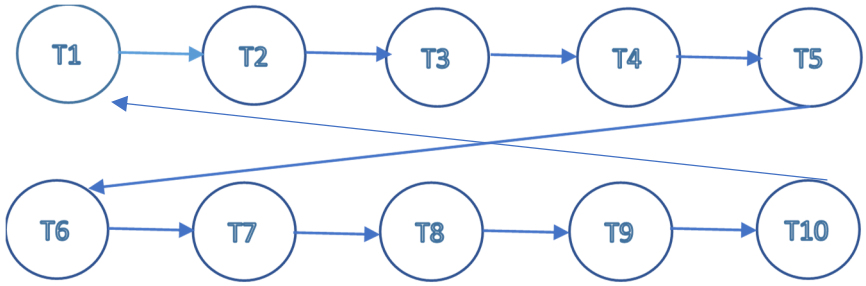

Рис. 1. Связанные состояния (этапы атаки) с учетом последовательности реализации

В графе присутствует связь состояний (как маркированных событий вредоносных воздействий). При распространении вектора атаки требуется условные распределения вероятностей сделать зависимыми только от предыдущего времени их фиксации:

$$\begin{aligned} P(y_3 \mid y_1, y_2) &= P(y_3 \mid y_2); \\ P(y_4 \mid y_1, y_2, y_3) &= P(y_4 \mid y_3); \\ P(y_n \mid y_1, \ldots, y_{n-1}) &= P(y_n \mid y_{n-1}). \end{aligned} \tag{1}$$

Далее классифицируются признаки событий, все случайные последовательности, которые соответствуют правилу марковской последовательности [2]:

$$P(y_1, \ldots, y_n) = P(y_1) \prod_{i=2}^{n} p(y_i \mid y_{i-1}), \tag{2}$$

где показатель y_{i-1} – предшествующее скомпрометированное состояние сетевого узла с фиксированным признаком атаки.

Процесс перехода из состояния (осуществленных тактик) в следующие состояния при соблюдении последовательностей на основе функциональной взаимосвязи описывается в виде дискретной марковской последовательности. Для выбранных периодов времени Δt вероятности перехода имеют вид [7]:

$$p_{ii}(t, t+\Delta t) = 1 - \lambda_{ii}(t) \cdot \Delta t + o(\Delta t),$$

$$p_{ij}\left(t, t+\Delta t\right) = \lambda_{ij}\left(t\right)\cdot\Delta t + o\left(\Delta t\right),\ i \neq j\ , \tag{3}$$

$\lambda_{ij}(t)$ – интенсивность перехода, характеризующая число переходов из состояния в новое состояние за определённый период.

Переходные вероятности p_{ij} в любой период времени t соответствуют простым линейным дифференциальным уравнениям [4]. При решении системы уравнений требуется внести начальные условия (начальные вероятности). Они выбираются с учетом специфики топологии систем и производимых атакующих воздействий [5]. Также необходимо ввести начальные условия, то есть вероятности присутствия во временной области реализации техники злоумышленника (в начальный период). При этом общая вероятность равна сумме начальных и условных вероятностей с учетом переходов в заданный момент [4].

Интенсивности переходов при следовании от одной тактики к другим зависят только от разности начального и переходного времени ($\tau = t - t_0$, т. е. $p_{ij}(t_o, t) = p_{ij}(\tau)$), и соответствуют формируемым дифференциальным уравнениям. Тогда задача сводится к решению системы дифференциальных уравнений вида [4]:

$$\frac{d}{dt} p_{ij}\left(\tau\right) = \sum_{g=1}^{G} \lambda_{ij}\left(t\right) p_{ij}\left(t\right). \tag{4}$$

На основании принципов построения марковских цепей формируется система уравнений, которая учитывает специфику зависимостей состояний (тактик), приводимых в Методике и описанных в графе (рис. 1), и интенсивность достижения состояний при осуществлении техник из начального состояния. Решение системы дифференциальных уравнений для разнообразных атакующих воздействий позволяет рассмотреть множество различных моделей атак с учетом того, что источником начальных состояний (начальных атакующий действий) является внешний нарушитель. Внутренний нарушитель становится актуальным при условии того, что часть информации уже ему известна, поэтому он может реализовать атакующие воздействия, используя промежуточные состояния (5).

Однако технология реализации атак не всегда предполагает четкую последовательность техник, приводимых в графе (рис. 1). Некоторые техники позволяют перейти к последующим тактикам без соблюдения обязательной последовательности переходов. Для определения подобных переходов нужно определить сопрягаемые техники различных тактик. В качестве критерия отбора связей для формирования модифицируемого графа используем следующий критерий: возможен ли переход без соблюдения последовательности техник, ближайших к рассматриваемому состоянию, в другие состояния, представленные другими техниками, и, соответственно, их тактиками [5]. Для этого требуется выделить те техники, которые позволяют осуществить подобный переход. Выявление подобных техник производится на основе сопоставления функций, которые в них заявлены. При этом предполагается, что результат одной функции можно использовать для реализации другой, принадлежащей к технике иной тактики, позволяющей получить новое состояние в графе компрометации.

$$\begin{cases} \frac{dP_{T1}}{dt} = \lambda_{1,10} P_{T10}(t) - \lambda_{12} P_{T2}(t) \\ \frac{dP_{T2}}{dt} = \lambda_{12} P_{T2}(t) - \lambda_{23} P_{T2}(t) \\ \frac{dP_{T3}}{dt} = \lambda_{23} P_{T3}(t) - \lambda_{34} P_{T3}(t) \\ \frac{dP_{T4}}{dt} = \lambda_{34} P_{T3}(t) - \lambda_{45} P_{T4}(t) \\ \frac{dP_{T5}}{dt} = \lambda_{45} P_{T4}(t) - \lambda_{56} P_{T5}(t) \\ \frac{dP_{T6}}{dt} = \lambda_{56} P_{T5}(t) - \lambda_{67} P_{T6}(t) \\ \frac{dP_{T7}}{dt} = \lambda_{67} P_{T6}(t) - \lambda_{78} P_{T7}(t) \\ \frac{dP_{T8}}{dt} = \lambda_{78} P_{T7}(t) - \lambda_{69} P_{T8}(t) \\ \frac{dP_{T9}}{dt} = \lambda_{89} P_{T8}(t) - \lambda_{9,10} P_{T10}(t) \\ \frac{dP_{T10}}{dt} = \lambda_{9,10} P_{T9}(t) - \lambda_{10,1} P_{T10}(t) \end{cases}. \quad (5)$$

На основе анализа функциональных взаимосвязей техник выделяются следующие связи тактик [1]:

1. Из состояния T1 техники позволяют перейти в состояние (задействовать) T2. Доступ получен стандартными способами, предусмотренными тактиками Методики.

2. Из состояния T2 техники позволяют перейти в состояние (задействовать) T3. Доступ получен стандартными способами, предусмотренными тактиками Методики.

3. Из состояния T2 техники позволяют перейти в состояния (задействовать) T4 и T5. Используются техники: T2.4, T2.8, T2.9, T2.10, T2.11, T2.13, T2.6, T2.7. Переход в состояние T4 обеспечен различными тактиками, в том числе теми, которые подразумевают использование ошибок конфигурации различного сетевого оборудования, а также средств фильтрации сетевого трафика. Это может быть выражено в компрометации паролей со слабым алфавитом или неизменённых и заданных по умолчанию ключевых данных, то есть логинов и пин-кодов. Кроме того, в состояние T5 можно перейти, используя недокументированные возможности программного обеспечения и оборудования, в том числе используя возможности, которые оставляют сами разработчики с целью последующей отладки или получения нелегитимного доступа для сбора информации о субъектах доступа. Переход в состояние T5 может быть обеспечен различными уязвимостями, связанными с легитимным использованием программного обеспечения. Злоумышленники могут использовать различные способы компрометации: средства перебора пароля, в том числе может производиться поиск устаревших, но всё ещё актуальных ключевых данных, что может приводить к компрометации легитимных данных пользователей компьютерных систем. Также могут быть использованы различные сетевые атаки, связанные с применением классического варианта вредоносного воздействия «человек посередине», в том числе с применением инфраструктур смежных организаций или открытых сетей. Все это позволяет, находясь в состоянии T2, обойти T3 и перейти в следующее состояние T4 или сразу перейти в состояние T5.

4. Из состояния T2 техники позволяют перейти в состояние (задействовать) T6. Для этого используются техники: T2.6, T2.8, T2.10. Они позволяют использовать недокументированные

возможности программного обеспечения и осуществить несанкционированный доступ к программному обеспечению от аккаунтов сотрудников.

5. Из состояния Т3 техники позволяют перейти в состояния (задействовать) Т4, Т6 и Т7. Для перехода в Т6 и Т7 используются техники: Т3.6, Т3.7, Т3.8, Т3.9, Т3.10. Тактики позволяют автоматическое создание вредоносных скриптов и использование таковых, включая подмену легитимных программных файлов, их библиотек, ссылок на легитимные программные библиотеки (допускается использование сетевых ресурсов, веб-ресурсов), а также позволяют использовать недокументированные возможности приложений и подмену дистрибутивов со встроенным вредоносным программным обеспечением (включая маскировку вредоносного программного обеспечения с помощью цифровых подписей).

6. Из состояния Т4 техники позволяют перейти в состояния (задействовать) Т5 и Т6. Для перехода в Т6 используются техники: Т4.1, Т4.2, Т4.3. Эти техники позволяют использовать несанкционированные возможности взломанных учётных записей при применении штатных средств удалённого доступа, также подразумевают скрытую установку средств удалённого доступа и перехвата управления операционной системой с учётом внесения изменений в ее конфигурацию и изменения в составе программно-аппаратных средств вычислительной системы.

7. Из состояния Т5 техники позволяют, кроме перехода в Т6, перейти в состояние (задействовать) Т9. Используются техники Т5.2, Т5.3, Т5.4 для перехода в Т9. Тактики подразумевают внедрение различных средств эксплуатации удалённых сервисов, а также использование протоколов верхнего уровня модели OSI с возможностью подключения к внешним серверам управления, обеспечивают перехват управления операционной системой с помощью данных внешних сервисов и управляемых ими вредоносных объектов, заражающих операционную систему.

8. Из состояния Т6 техники позволяют перейти не только в состояния (задействовать) Т7, но и в Т8, Т9, Т10. Для этого используются техники Т6.1, Т6.2, Т6.3. Эти тактики используют сеть и подразумевают получение доступа к другим компьютерным системам. В частности, тактики подразумевают эксплуатацию уязвимостей программного обеспечения системного и пользовательского типа, подбор паролей к административным учётным записям, а также использование различных привилегированных аккаунтов. Также может использоваться перехват сессионных ключей.

9. Из состояния Т7 техники позволяют перейти в состояние (задействовать) Т8. Доступ получен стандартными способами, предусмотренными тактиками Методики.

10. Из состояния Т8 техники позволяют перейти не только в состояние (задействовать) Т9, но и в Т10. Тактики позволяют выводить данные из компьютерной системы различными способами, в том числе скрытыми, организовать криптографические каналы для выемки данных из атакованных узлов.

11. Из состояния Т9 техники позволяют перейти в состояние (задействовать) Т10. Доступ получен стандартными способами, предусмотренными тактиками Методики.

12. Состояние Т10 подразумевает достижение цели злоумышленником и переход к новой атакующей последовательности, то есть к состоянию Т1. Также повтор атакующей последовательности может произойти в результате полного краха атаки на последнем этапе.

Таким образом, приведенные тактики подразумевают множество вариантов атакующих воздействий и позволяют достичь состояния, которое определяется как тактика № 10, то есть состояния, подразумевающего успешность атаки. При этом не требуется обязательно соблюдать последовательность приводимых в Методике тактик, то есть техники позволяют некоторые этапы обходить. На основании приведённого анализа формируется граф атаки (рис. 2). Часть его вершин будет возможно обойти исходя из специфики техник и тактик, другие же вершины будут совмещать множество входящих дуг (переходов), тем самым аккумулируя вероятности переходов.

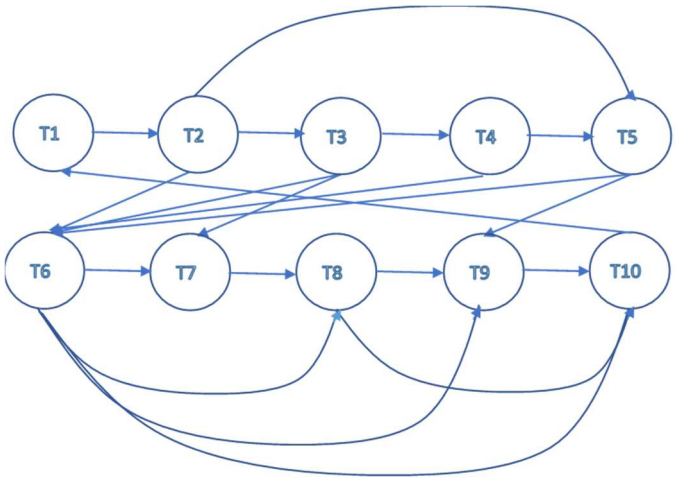

Рис. 2. Модифицированный граф состояний с учетом последовательности реализации

Модифицированный граф состояний с учетом выявленных особенностей в последовательности реализации тактик можно описать системой дифференциальных уравнений, на основании которых осуществляется оценка вероятностей перехода из начальных состояний в новые состояния:

$$\begin{cases} \frac{dP_{T1}}{dt} = \lambda_{1,10}P_{T10}(t) - \lambda_{12}P_{T2}(t) \\ \frac{dP_{T2}}{dt} = \lambda_{12}P_{T2}(t) - \lambda_{23}P_{T2}(t) - \lambda_{26}P_{T2}(t) \\ \frac{dP_{T3}}{dt} = \lambda_{23}P_{T3}(t) - \lambda_{34}P_{T3}(t) - \lambda_{36}P_{T3}(t) - \lambda_{37}P_{T3}(t) \\ \frac{dP_{T4}}{dt} = \lambda_{34}P_{T3}(t) - \lambda_{45}P_{T4}(t) \\ \frac{dP_{T5}}{dt} = \lambda_{25}P_{T2}(t) + \lambda_{45}P_{T4}(t) - \lambda_{56}P_{T5}(t) - \lambda_{59}P_{T5}(t) \\ \frac{dP_{T6}}{dt} = \lambda_{26}P_{T2}(t) + \lambda_{36}P_{T4}(t) + \lambda_{46}P_{T4}(t) + \lambda_{56}P_{T4}(t) - \lambda_{67}P_{T6}(t) \\ -\lambda_{68}P_{T6}(t) - \lambda_{69}P_{T6}(t) - \lambda_{6,10}P_{T6}(t) \\ \frac{dP_{T7}}{dt} = \lambda_{67}P_{T6}(t) + \lambda_{37}P_{T3}(t) - \lambda_{78}P_{T7}(t) \\ \frac{dP_{T8}}{dt} = \lambda_{78}P_{T7}(t) + \lambda_{68}P_{T6}(t) - \lambda_{89}P_{T6}(t) - \lambda_{8,10}P_{T6}(t) \\ \frac{dP_{T9}}{dt} = \lambda_{89}P_{T8}(t) + \lambda_{69}P_{T6}(t) + \lambda_{79}P_{T7}(t) - \lambda_{9,10}P_{T10}(t) \\ \frac{dP_{T10}}{dt} = \lambda_{8,10}P_{T8}(t) + \lambda_{9,10}P_{T9}(t) - \lambda_{10,1}P_{T10}(t) \end{cases}. \quad (6)$$

Из приведенной системы видно, что специфика связей предполагает множество различных сопряжений и взаимных влияний параметров вероятностей переходов, что приводит к усложнению вычислений. На основании сопряжения функции возможно упростить граф, используя приведённые вычисления. В графе (рис. 2) можно отметить, что состояния Т6 является результатом переходов из состояний Т2, Т3, Т4, Т5. Таким образом, можно упростить решение

задач вычисления переходных вероятностей, представив часть графа (Т2, Т3, Т4, Т5) в виде свёртки (рис. 3).

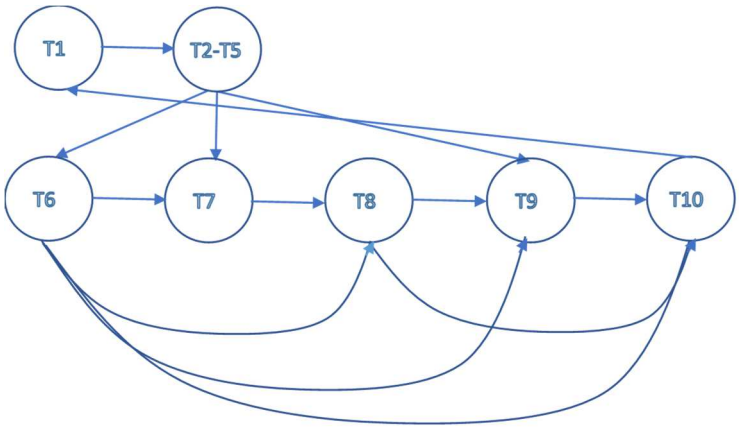

Рис. 3. Сокращенный модифицированный граф состояний с учетом последовательности реализации

Сокращенный модифицированный граф состояний с учетом последовательности реализаций тактик описывается иной системой дифференциальных уравнений:

$$\begin{cases} \frac{dP_{T1}}{dt} = \lambda_{1,10}P_{T10}(t) - \lambda_{12}P_{T2}(t) \\ \frac{dP_{T2}}{dt} = \lambda_{12}P_{T2}(t) - \lambda_{27}P_{T2}(t) - \lambda_{26}P_{T2}(t) - \lambda_{29}P_{T2}(t) \\ \frac{dP_{T6}}{dt} = \lambda_{26}P_{T2}(t) - \lambda_{67}P_{T6}(t) - \lambda_{68}P_{T6}(t) - \lambda_{69}P_{T6}(t) - \lambda_{6,10}P_{T6}(t) \\ \frac{dP_{T7}}{dt} = \lambda_{67}P_{T6}(t) + \lambda_{27}P_{T2}(t) - \lambda_{78}P_{T7}(t) \\ \frac{dP_{T8}}{dt} = \lambda_{78}P_{T7}(t) + \lambda_{68}P_{T6}(t) - \lambda_{68}P_{T6}(t) - \lambda_{69}P_{T6}(t) \\ \frac{dP_{T9}}{dt} = \lambda_{89}P_{T8}(t) + \lambda_{69}P_{T6}(t) + \lambda_{29}P_{T2}(t) - \lambda_{9,10}P_{T10}(t) \\ \frac{dP_{T10}}{dt} = \lambda_{8,10}P_{T8}(t) + \lambda_{9,10}P_{T9}(t) - \lambda_{10,1}P_{T10}(t) \end{cases} . \quad (7)$$

Очевидно, что количество вычислений, требуемых для расчёта переходных вероятностей сокращенного графа, стало меньше. Кроме того, с учётом упрощения графа точность рассчитываемых переходных вероятностей может падать, если переходы между состояниями Т2, Т3, Т4, Т5 должны присутствовать обязательно. Это определяется исходя из специфики атаки.

Моделирование атак типа «спуфинг» (при использовании аппарата марковских цепей и тактик Методики ФСТЭК) предполагает рассмотрение упрощенного графа (рис. 3) с изъятием состояния Т9, так как его тактики не используются при достижении Т10. Поэтому систему уравнений вероятности переходов (7) можно еще более упростить.

Определим стационарные характеристики процесса, описывающего действия злоумышленника при реализации атаки. Учитывая статистику отраженных и реализованных атак, а также опыт технической эксплуатации защищенных распределенных систем, в качестве переходных вероятностей были приняты следующие значения [10]:

$$\Pi = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.3 & 0 & 0 & 0.7 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.9 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (8)$$

В качестве распределений времени пребывания в состояниях принято экспоненциальное распределение со следующей матрицей интенсивностей переходов:

$$\Lambda = \begin{pmatrix} 0 & 0.005 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.005 & 0 & 0 & 0.2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.4 & 0 & 0.008 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.008 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.05 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (9)$$

По итогам расчетов на основе предложенной модели (с учетом числа и специфики тактик сокращённого графа) были получены стационарные вероятности пребывания в каждом из состояний рассматриваемого графа: [0.469; 0.147; 0.023; 0; 0; 0.341; 0; 0.289; 0; 0.041]. В то же время по итогам расчетов при использовании полного графа стационарные вероятности несколько отличаются от предыдущих значений: [0.56; 0.15; 0.016; $4.68 \cdot 10^{-5}$; 0.047; 0.103; $2.31 \cdot 10^{-4}$; 0.045; 0.4; 0.21; 0.055].

Расхождения в значениях вероятностей присутствуют, хотя они минимальны в конечных состояниях, советующих тактике Т10, и в большей степени наблюдаются на промежуточных этапах развития атаки. Это объясняется влиянием исключенных из сокращённого графа и присутствующих в полном графе тактик: их значения обновляются при каждой итерации. Незначительная величина расхождения состояний Т10 обоих графов объясняется минимальным влиянием техник Т3, Т4, Т5, Т9 при реализации технологии атак типа «спуфинг».

4. Заключение

Таким образом, при определении вектора атаки в дополнение к способам, изложенным в методических документах ФСТЭК, можно использовать марковские последовательности. Их применение представлено в виде двух реализаций: полного графа со всеми функциональными взаимосвязями и сокращенного, включающего в свой состав свёртку вероятностей переходов с Т2 по Т5.

При моделировании следуют учитывать требуемую при аудите, анализе угроз и уязвимостей точность. При этом оба подхода могут дать представление об изменении состояния безопасности системы. Граф с полным набором состояний можно применять для расследования инцидентов, проверки гипотез о компрометации ресурсов систем. Граф с сокращенным набором состояний можно применять при отслеживании развертывания атак для быстрого определения конечного направления атакующих действий (конечных целей) злоумышленника.

Литература

1. Методика оценки угроз безопасности информации Методический документ ФСТЭК России: утв. ФСТЭК России 5 февраля 2021 г.
2. ГОСТ Р 56546-2015 Национальный стандарт российской федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. М.: Стандартинформ, 2018 г.
3. *Горбачев И. Е., Глухов А. П.* Моделирование процессов нарушения информационной безопасности критической инфраструктуры// Труды СПИИРАН. 2015. Вып. 1 (38). С. 112–135.
4. *Котенко И. В., Саенко И. Б., Лаута О. С., Крибель А. М.* Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Первая миля. 2021. № 6. С. 64–71.
5. *Добрышин М. М.* Модель разнородных компьютерных атак, проводимых одновременно на узел компьютерной сети связи // Телекоммуникации. 2019. № 12. С. 31–35.
6. *Канаев А. К., Опарин Е. В., Опарина Е. В.* Обобщенная модель действий злоумышленника при манипулировании сообщениями, содержащими сигналы точного времени // T-Comm. 2022. Т. 16, № 6.
7. *Петров М. Ю., Фаткиева Р. Р.* Модель синтеза распределенных атакующих элементов в компьютерной сети // Труды учебных заведений связи. 2020. Т. 6, № 2. С. 113–120. DOI:10.31854/ 1813-324X-2020-6-2-113-120.
8. *Щеглов А. Ю.* Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и Техника, 2004. 384 с.
9. *Галатенко В. А.* Управление рисками: обзор употребительных подходов (часть 2) // Jet Info. 2018. № 12.
10. Canadian Institute for Cybersecurity: NSL-KDD dataset [Электронный ресурс]. URL: `https://www.unb.ca/cic/datasets/nsl.html` (дата обращения: 17.05.2020).

Ветров Игорь Анатольевич

к.т.н., доцент, ОНК «Институт высоких технологий», Балтийский федеральный университет им. И. Канта (236041, Калининград, ул. Александра Невского, 14), e-mail: `vetrov.gosha2009@yandex.ru`, ORCID ID: 0000-0002-3189-9085.

Подтопельный Владислав Владимирович

старший преподаватель, Институт цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» (236022, Калининград, Советский пр., 1), e-mail: `ionpvv@mail.ru`, ORCID ID: 00000-0002-7618-3224.

Авторы прочитали и одобрили окончательный вариант рукописи.

Авторы заявляют об отсутствии конфликта интересов.

Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Formation of the network attack vector taking into account the connections specifics of techniques and tactics

Igor A. Vetrov[1], Vladislav V. Podtopelny[2],

[1] Immanuel Kant Baltic Federal University (IKBFU)
[2] Kaliningrad State Technical University (KSTU).

Abstract: The problems arising with the tasks of constructing an attack vector in a network infrastructure are considered. The varieties of various tactics and techniques of FSTEC techniques used in the construction of a network attack vector are presented and characterized as well as the specifics of their interrelations with the use of Markov chains in the modeling of attacking influences, their suitability for various procedures for determining vector parameters. When constructing a network attack vector, the features of determining the probabilities of system transitions to various states of network compromise are considered. The formation of the attack vector is studied taking into account the specifics of the multilevel organization of the corporate information system. The features of the construction of a simplified vector are determined taking into account the specifics of tactical relationships (states).

Keywords: attack vector, information system, corporate network, vulnerability, Markov processes, intruder, tactics.

For citation: Vetrov I. A., Podtopelny V. V. Formation of the network attack vector taking into account the connections specifics of techniques and tactics (in Russian). *Vestnik SibGUTI*, 2023. vol. 17, no. 4. pp. 49-61. https://doi.org/10.55648/1998-6920-2023-17-4-49-61.

The article was submitted: 25.05.2023;
accepted for publication 07.06.2023.

References

1. *Metodika otsenki ugroz bezopasnosti informatsii Metodicheskii dokument FSTEK Rossii: utv. FSTEK Rossii 5 fevralya 2021.* [Methodology for assessing threats to information security Methodological document of the FSTEC of Russia]. Moscow, 2021.
2. *GOST R 56546-2015 Natsional'nyi standart rossiiskoi federatsii. Zashchita informatsii. Uyazvimosti informatsionnykh sistem. Klassifikatsiya uyazvimostei informatsionnykh system* [National Standard of the Russian Federation. Data protection. Vulnerabilities of information systems. Classification of vulnerabilities of information systems]. Moscow, Standartinform, 2018.
3. Gorbachev I. E., Glukhov A. P. Modelirovanie protsessov narusheniya informatsionnoi bezopasnosti kriticheskoi infrastruktury [Modeling the processes of violation of information security of critical infrastructure]. *Trudy SPIIRAN*, Moscow, 2015, iss. 1(38), pp. 112 – 135.
4. Kotenko I. V., Saenko I. B., Lauta O. S., Kribel' A. M. Metod rannego obnaruzheniya kiberatak na osnove integracii fraktal'nogo analiza i statisticheskih metodov [Method for early detection of cyber-attacks based on the integration of fractal analysis and statistical methods]. *Pervaya milya*, 2021, no. 6, pp. 64-71.
5. Dobryshin M. M. Model' raznorodnyh komp'yuternyh atak, provodimyh odnovremenno na uzel komp'yuternoj seti svyazi [Model of heterogeneous computer attacks carried out simultaneously on a computer communication network node]. *Telekommunikacii*, 2019, no. 12, pp. 31-35.

6. Kanaev A. K., Oparin E. V., Oparina E. V. Obobshchennaya model' dejstvij zloumyshlennika pri manipulirovanii soobshcheniyami, soderzhashchimi signaly tochnogo vremeni [A generalized model of an attacker's actions when manipulating messages containing precise time signals]. *T-Comm*, vol.16, no. 6, 2022.
7. Petrov M. YU., Fatkieva R. R. Model' sinteza raspredelennyh atakuyushchih elementov v komp'yuternoj seti [Model for the synthesis of distributed attack elements in a computer network]. *Trudy uchebnyh zavedenij svyazi*. 2020, vol. 6, no. 2, pp. 113-120. DOI:10.31854/ 1813-324X-2020-6-2-113-120.
8. Shcheglov A. YU. *Zashchita komp'yuternoj informacii ot nesankcionirovannogo dostupa* [Protecting computer information from unauthorized access]. Saint Petersburg, Nauka i Tekhnika, 2004. 384 p.
9. Galatenko V. A. Upravlenie riskami: obzor upotrebitel'nykh podkhodov (chast' 2) [Risk management: a review of common approaches (part 2)]. *Jet Info*, no. 12, 2018, available at: https://www.jetinfo.ru/upravlenie-riskami-obzor-upotrebitelnykh-podkhodovchast-2/ (accessed: 29.01.2022).
10. Canadian Institute for Cybersecurity: NSL-KDD dataset, 2009. available at: https://www.unb.ca/cic/datasets/nsl.html (accessed: 17.05.2020).

Vetrov Igor A.

Cand. of Sci. (Engineering), Associate Professor, Institute of High Technologies, I. Kant Baltic Federal University (236041, Kaliningrad, Alexander Nevsky Str., 14), e-mail: vetrov.gosha2009@yandex.ru, ORCID ID: 0000-0002-3189-9085.

Podtopelny Vladislav V.

Senior lecturer, Institute of Digital Technologies of KSTU (236022, Kaliningrad, Sovetsky ave., 1), e-mail: ionpvv@mail.ru, ORCID ID: 00000-0002-7618-3224.