УДК 004.056.5:378.3
DOI: 10.55648/1998-6920-2022-16-3-3-13

Особенности формирования вектора современных сетевых атак

И. А. Ветров, В. В. Подтопельный

Рассмотрены проблемы, возникающие при постановке задачи определения вектора сетевой атаки в корпоративной информационной сети. Приведены и охарактеризованы разновидности методик, упрощающих построение вектора сетевой атаки, применяемых при анализе надежности информационных систем, рассмотрена их пригодность для различных процедур определения параметров вектора. При построении вектора сетевой атаки определяется специфика проявления параметра времени как характеристики, указывающей на более эффективный путь распространения компрометации. Формирование вектора рассматривается с учетом специфики многоуровневой организации сетей. Определяется специфика упрощенной модели вычисления вектора, которая включает процедуры, ориентированные на различные подходы.

Ключевые слова: вектор сетевой атаки, информационная система, корпоративная информационная сеть, уязвимость.

1. Введение

Для построения вектора атаки в Российской Федерации применяются несколько руководящих документов, последний из которых принят в 2021 году – «Методика оценки угроз безопасности информации» (далее – Методика). Приведенная в нём методика предлагает использовать при определении тактики злоумышленника массивы данных о признаках угроз, об уязвимостях, а затем, ориентируясь на экспертное мнение, формировать векторы атак с возможностью заимствования различных, в том числе зарубежных, способов описания сценариев реализации угрозы (CAPEC, ATT&CK, OWASP, STIX, WASC и др.) [1]. В данном документе при построении вектора предполагается учитывать угрозы, потенциал возможных нарушителей (уровень их квалификации, наличие средств атаки, а также предложено рассмотреть аспекты целеполагания нарушителей).

Приведённая методика направлена на рассмотрение в качестве целевого объекта распределенных информационных систем, построенных на клиентско-серверной архитектуре, но при этом не исключается рассмотрение локальных систем (они не предполагают применения сетевых технологий для поддержи работоспособности системных и пользовательских компонентов). Очевидно, что типы информационных систем и специфика поиска уязвимостей в этих информационных системах должны быть учтены при построении векторов атак по требованиям рассматриваемого методического документа. Однако в самой методике хотя и используются понятия риск (фактически подразумевается прогноз возможных действий злоумышленника), угроза, специфика классификации признакового пространства сетевых атак не учитывается, а построение последовательности тактик основано на экспертной оценке, которая зачастую неточна из-за субъективности оценок экспертов. Кроме того, сам предложенный способ описания вектора атаки не подразумевает формального учёта вероятностных показателей путей достижения цели злоумышленником (вероятность достижения цели злоумышленником

одним из путей предполагает наличие наиболее эффективного – быстрого и гарантированного – способа эксплуатации актуальных уязвимостей). Соответственно, для более точного построения сценария атаки, предложенную Методику требуется дополнить простыми (то есть не вызывающими затруднения при применении на производстве при построении модели угроз) формальными способами определения последовательности вредоносных воздействий (тактик).

2. Проблемная область формирования вектора атаки

Вектор атаки должен учитывать возможность возникновения нового направления атакующих воздействий или нового сценария реализации угрозы. Таким образом, вектор, построенный с учетом факторов, изменяющих направление атаки (в том числе с применением средств защиты), будет включать некоторое количество сегментов вектора, описываемых как состояния с признаками компрометации, признаками эксплуатации уязвимостей (несанкционированного доступа (НСД) на одном узле, на множестве узлов) [2]. Подобный способ формирования вектора выгоден при реализации аудита многоуровневых систем, поскольку в этом случае будут учитываться все особенности используемых при обработке информации технологий, особенности средств защиты. Продолжение вектора или определение нового направления вектора будет зависеть от меры успешности предыдущих атакующих последовательностей. При описании вектора в Методике предлагается использовать мнение экспертов, которые должны участвовать в обсуждении проблем безопасности и оценивании способов реализации различных угроз.

При сегментировании подсистем оцениваемых АИС и, соответственно, при использовании процедур поиска угроз и уязвимостей может проявиться проблема несогласованности оценок различных групп экспертов, занимающихся анализом своих профильных подсистем и компонентов технологически различающихся уровней одной информационной системы, что затрудняет определение направления вектора атаки при множестве данных о состоянии безопасности.

Некоторые сетевые параметры могут определяться как маркеры атаки только тогда, когда они используются совместно с другими маркерами или при определенных условиях их (маркеров) проявления. При этом их фиксация может указывать на простую ошибку передачи данных в сети. Таким образом, само выявление сигнатурных маркеров в некоторых случаях не гарантирует того, что выстроенный вектор атаки соответствует реалиям атакующих воздействий. Более того, повышается вероятность получения ошибочных сетевых пакетов при работе в сетях большого масштаба, а также при некорректной настройке маршрутизирующих устройств. Допустим, в векторе атак сегментов и уровней АСУТП признаки атаки следующие: запрос к закрытым портам сетевых служб; ошибочная последовательность флагов TCP при открытии соединения или в ходе соединения, множественная попытка открытий соединений в ограниченный период времени, неправильные контрольные суммы пакетов транспортных протоколов, IP-адрес сетевого узла назначения совпадает с IP-адресом источника, последовательный опрос портов. Последний параметр нельзя отнести к явным признакам атаки, так как он зависит от периодичности нагрузок на трафик [4]. Более того, сетевые атаки в своей сигнатурной последовательности могут включать больший массив признаков нормального трафика по сравнению с однозначно маркирующими класс атаки признаками или включать признаки других атак, что приводит к путанице при их классификации (рис. 1). Стандартно к параметрам, которые однозначно (явно) маркируют присутствие вредоносной активности или ошибочная интерпретация которых наименее вероятна, можно отнести:

1. Наборы флагов, которые не соответствуют стандарту соединения по TCP-протоколу (RFC-793).

2. Наличие в TCP-пакете порта узла-источника, равного 0 (нельзя использовать нулевой порт).

3. Несоответствие указанных контрольных сумм пакетов их оригинальным суммам.

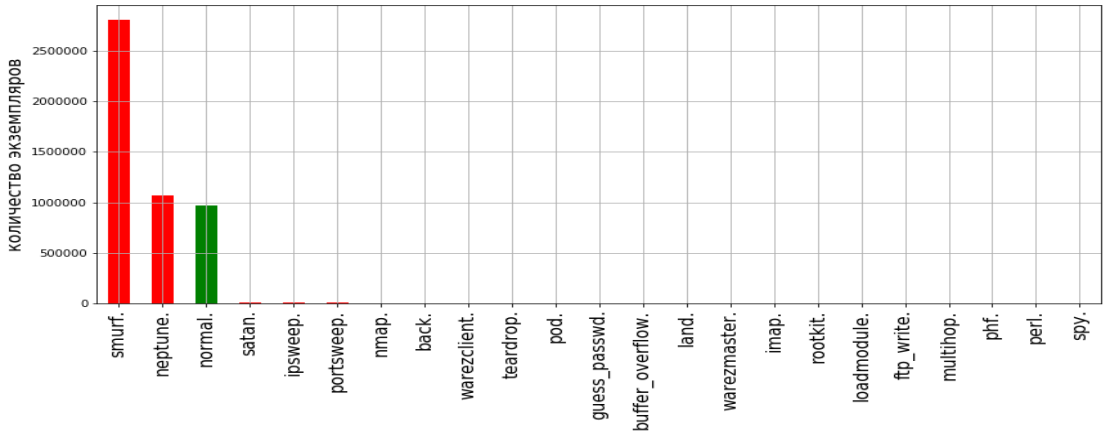

Рис. 1. Гистограмма распределения экземпляров данных

Таким образом, среди маркеров сетевых атак, позволяющих создать признаковое пространство, можно выделить два типа: явные и косвенные. Очевидно, что не все косвенные маркеры можно игнорировать. Однако при намеренном учете в правилах всех косвенных признаков вероятность ошибки при определении атаки будет возрастать. Соответственно, первоначально требуется при построении вектора атаки учитывать однозначно интерпретируемые признаки вредоносный действий. Общее представление о признаках, позволяющих различать классы атак на транспортном уровне OSI, приведено в табл. 1.

Таблица 1. Факторы (признаки), позволяющие различать векторы атак, которые распространяются параллельно в одной сетевой инфраструктуре

Данные, которые постоянно встречаются при анализе	Уникальные данные, которые следует учитывать в отдельных случаях
1. Количество принятых сетевых пакетов. 2. Число TCP-пакетов с ACK-флагом. 3. Число TCP-пакетов с SYN- флагом. 4. Число TCP-пакетов с FIN- флагом. 5. Время жизни сетевого пакета (TTL). 6. Число ICMP-пакетов. 7. Общее количество пакетов TCP. 8. IP-адреса сетевых узлов. 9. Длина сетевого пакета.	1. Число ICMP-ответов без ICMP-запросов. 2. Количество запросов с неправильными комбинациями флагов. 3. IP-адрес и MAC-адрес в ARP-reply. 4. Запросы к закрытым портам. 5. Пакеты опроса портов. 6. TCP-пакеты с портом источника 0. 7. Количество открытий соединений. 8. Число полуоткрытых соединений. 9. Число UDP-пакетов.

Чтобы снизить большое количество ложных срабатываний систем обнаружения вторжений (СОВ), требуется математическими методами скорректировать формируемый вектор атаки. На рис. 1 видно, что большая часть признаков атак имеет малый масштаб фиксации по сравнению с первыми атаками на диаграмме (показано красным цветом). Соответственно, при эксплуатации системы обнаружения вторжений плохо интерпретируемые сетевые атаки (с малым пулом данных) сложно распознавать с большой достоверностью при поведенческом и эвристическом анализе. При этом СОВ остаётся работоспособной и может отсеивать большой массив других атак [5].

Одним из способов построения вектора атаки является использование графа компрометации. В данном графе ребрами обозначаются соответствующие переходы (при эксплуатации уязвимостей) между состояниями компрометации следующих типов: зондирование, взлом, проникновение, эскалация, нанесение ущерба. Граф предполагает изменение направления

атаки в зависимости от наличия или отсутствия информации об уязвимостях системы и средств их эксплуатации. Показатель успешности атаки определяется по формуле [6]:

$$T = t_1 \cdot P_1 + P_2 \cdot (1 - P_1) \cdot t_2 + (1 - P_1) \cdot (1 - P_2) \cdot t_3, \quad (1)$$

где t_1 – ожидаемое время успешного завершения атаки при известности уязвимостей и средств их эксплуатации (обычно 1 день);

t_2 – ожидаемое время завершения атаки при неизвестности уязвимостей;

P_1 – вероятность успешного завершения атаки при известности уязвимостей и средств их эксплуатации;

P_2 – вероятность успешного завершения атаки при неизвестности уязвимостей [6].

Поскольку при рассмотрении корпоративных информационных систем (КИС) выделяются множества различных параллельно и последовательно связанных объектов, векторы атак необходимо представить при учете сегментированных подсистем, классифицируемых по специфике их функционального предназначения. Таким образом, выстраивается последовательность вероятностей проявления вредоносных воздействий, ассоциированных с конкретными элементами КИС. Это позволит локализовать узкие места в проекте КИС или определить при предварительном анализе область нахождения причины сбоев [7].

Другой подход к формированию предполагает формирование вектора на основе переходов в логическом отображении сетевой инфраструктуры организации исследуемых систем (топологический принцип), его можно привести в виде набора элементов нескольких множеств (элементы имеют различные взаимосвязи), которые и следует учитывать при разработке модели компрометации (рис. 2). Выделяются следующие типы множеств [8]:

– множество объектов узлов (U);

– множество потенциальных угроз проявления аномалий (A);

– множество средств ИБ, модифицирующих вектор атак (R).

При этом наборы векторов аномалий будут включать каждую ветку направленного графа распространения, вершинами которого будут являться элементы описанных множеств.

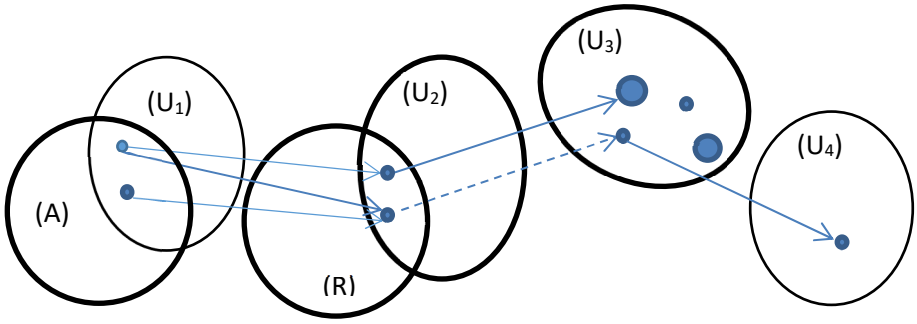

Рис. 2. Граф распространения вектора атаки со множествами сетевых узлов-вершин с учетом времени и альтернативного пути

Оба подхода не позволяют достоверно отобразить вектор развертываемой атаки с учетом всех особенностей. В первом случае применение топологических характеристик необязательно, а во втором случае не предполагается вычисление вероятностей переходов от одного узла к другому. Соответственно, требуется рассмотреть и совместить подходы, представляющие граф компрометации, то есть вектор атаки, как фиксацию признаков присутствия угрозы (состояния небезопасности на последовательности узлов) и граф компрометации как набор этапов, каждый из которых указывает на продвижение злоумышленника к цели своей атаки с определённой скорость (временем достижения состояния компрометации).

3. Построение вектора и определение скорости его распространения

Для построения вектора есть последовательность состояний, которые реализуются в виде последовательно фиксируемых признаков атаки на сетевых узлах с учетом времени фиксации признаков. Модернизированный граф с учетом времени и состояний компрометации формируется в контексте массива сходных атакующих воздействий (атаки со множеством способов реализации), при этом в каждом случае предполагается различная скорость достижения целей злоумышленника, что влияет на приоритет ветви вектора при выборе сценария атаки, а значит, позволяет определить его актуальность. Таким образом, ключевым параметром в описании вектора является время достижения некоторого компрометированного состояния, выраженного в виде ранее неактивного однозначно интерпретируемого признака атаки (набора признаков атаки). Описание этого признака – нетривиальная задача. Допустим, при анализе вектора сетевой разведки описание параметра времени компрометации резко осложняется неравномерной зависимостью скорости сканирования от количества портов тестируемого сетевого узла. В табл. 2 можно увидеть сильный разброс значений времени отклика при полуоткрытом SYN-сканировании с помощью утилиты Nmap. На показатели сканирования могут влиять следующие факторы [5]:

- показатель загрузки трафика в сети в период сканирования;
- пропускная способность сетевого интерфейса;
- количество Nmap-пакетов в сети в заданный период времени.

Таблица 2. Результаты полуоткрытого SYN-сканирования

№ раунда (эксперимента)	число портов	среднее значение, с.	1 скан.	2 скан.	3 скан.	4 скан.	5 скан.	6 скан.	7 скан.	8 скан.	9 скан.
1	1	0.63	0.63	0.65	0.62	0.62	0.63	0.64	0.61	0.63	0.65
2	10	1.82	1.82	1.82	1.80	1.83	1.86	1.82	1.82	1.80	1.79
3	100	2.05	2.04	2.06	2.05	2.04	2.07	2.05	2.05	2.04	2.04
4	250	2.37	2.43	2.40	2.30	2.25	2.40	2.40	2.32	2.41	2.43
5	500	5.45	6.21	6.20	6.20	3.16	6.19	3.11	3.14	3.14	11.71
6	750	7.83	9.20	8.61	8.60	8.00	7.81	7.69	7.82	4.10	8.60
7	1000	19.91	33.71	11.89	9.49	11.11	11.12	9.49	35.37	21.80	35.25
8	1500	27.54	14.23	16.53	16.75	34.12	14.21	16.52	49.80	45.27	40.45
9	2000	54.58	18.32	90.14	41.97	37.50	71.81	13.21	74.13	84.42	59.74

Присутствует смешение параметров-признаков угроз, и часть из представленных признаков с учетом фиксации времени их проявления становится белым шумом, если система не ориентирована четко дифференцировать векторы с учетом вредоносных операций (действий злоумышленника). Фиксируемые признаки можно представить в виде случайной дискретной последовательности длиной n отсчетов:

$$Y = [y_1, y_2, y_3, \ldots, y_n]. \tag{2}$$

Можно вероятностно описать с помощью многомерной плотности распределения вероятностей (a):

$$a(y_1, y_2, y_3, \ldots, y_n) = a(y_1) \cdot a(y_2 \mid y_1) \cdot a(y_3 \mid y_1, y_2) \cdot \ldots \cdot a(y_n \mid y_1, \ldots, y_{n-1}). \tag{3}$$

Но очевидно, что все параметры, фиксируемые подобным образом, будут независимыми между собой, что в рамках поля фиксируемых признаков будет смешение ложных признаков (рис. 3) и признаков отслеживаемой атаки (выделен на рис. 3 оранжевым цветом).

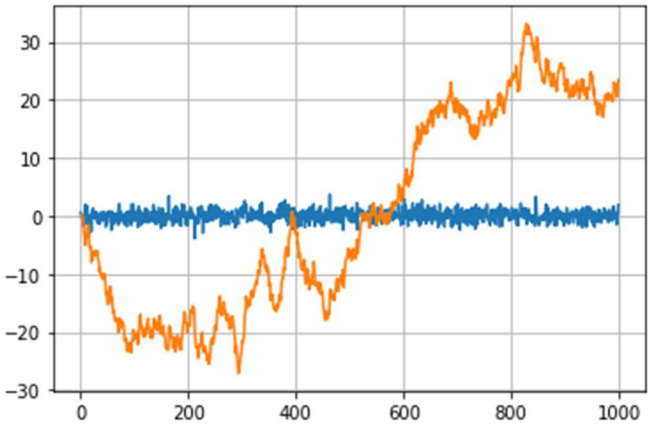

Рис. 3. Множества признаков вектора атаки

Тогда для того, чтобы представить связь признаков вредоносных воздействий (как фиксации состояния компрометации) при распространении вектора атаки, требуется условные распределения вероятности сделать зависимыми только от предыдущего момента их фиксации:

$$a(y_3 \mid y_1, y_2) = a(y_3 \mid y_2);$$
$$a(y_4 \mid y_1, y_2, y_3) = a(y_4 \mid y_3);$$
$$a(y_n \mid y_1, \ldots, y_{n-1}) = a(y_n \mid y_{n-1}).$$

Далее, классифицируя признаки атаки, все случайные последовательности, которые соответствуют правилу, выраженному в марковской последовательности, можно выразить следующим образом [9]:

$$a(y_1, \ldots, y_n) = a(y_1) \prod_{i=2}^{n} a(y_i \mid y_{i-1}),\ y_i = y_{i-1} + \xi_i, \tag{4}$$

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

ξ_i – случайное изменение как величина нормальной плотности распределения вероятностей с нулевым математическим ожиданием и дисперсией σ_ξ^2.

Таким образом, типовой вектор атаки (то есть определение направления) можно наложить на сетевую топологию (требуется учитывать свёртки графа, если несколько признаков последовательно фиксируется на одном узле), чтобы получить последовательность и прогноз следующего шага нарушителя с учетом времени переходов от одного локализованного состояния компрометации к другому. Соответственно, можем определить все условные плотности распределения вероятностей переходов следующим образом:

$$a(y_i \mid y_{i-1}) = \frac{1}{\sigma_\xi \sqrt{2\pi a}} \cdot \exp\left(-\frac{\sigma_\xi}{2\sigma_\xi^2} \right), \tag{5}$$

Таким образом, можно произвести прогнозирование изменения вектора атаки и, соответственно, построить алгоритм ее реализации.

Формируемый вектор будет состоять из вершин, фиксируемых при переходах систем из одного состояния компрометации в типологически отличное следующие. Для коррекции роста дисперсии не требуется дополнительных вычислений, так как количество переходов в графе для корпоративных сетей мало и, соответственно, разброс величин (вероятностей отклонения вектора атаки) мал. При рассмотрении версий атакующих воздействий с учетом возможностей злоумышленника (два дополнительных варианта развития событий по графу компрометации) можно использовать типы этапов графа компрометации, при этом вычисляя время атаки с применением марковских последовательностей.

Тогда возникает пять основных множеств признаков при расчете временных показателей по числу типов переходов в графе компрометации (множество признаков состояний зондирования, взлома, проникновения, эскалации, нанесения ущерба) или десять в соответствии с типовыми тактиками Методики (множество признаков успешной реализации массива техник, принадлежащих к классам последовательно примененных тактик), что в итоге можно использовать при настройке средств защиты, ориентированных на определенные методы воздействия нарушителя. Для масштабных интернет-топологий с большим количеством узлов или состояний компрометации требуется скорректировать величину дисперсии, применив авторегрессии 1-го порядка (нужно добавить случайную величину с дисперсией).

Используя векторные марковские последовательности можно рассмотреть два типа векторов:

1. Первый тип с учетом состояний компонентов сети (по графу, по Методике) и времени, затрачиваемого на достижения этих состояний (t_i). При этом компоненты объединены по множеству типов воздействия и наличию признаков атаки (y_i). И для каждой из координат состояния компрометации можно записать модель:

$$\begin{cases} y_i = y_{i-1} + \xi_{ti} \\ t_i = t_{i-1} + \xi_{ti} \end{cases}. \quad (6)$$

На рисунках ниже изображены примеры векторов атаки с учетом состояний компрометации (рис. 4) и с учетом фиксации признаков проявления тактик злоумышленника (рис. 5). Вектор включает в свой состав порядок действий (фиксацию из признаков), характерный для следующих типов атакующих воздействий:

1. Сетевая разведка (сканирование Nmap, сниффинг).
2. ARP-спуфинг.
3. Перехват сеанса.

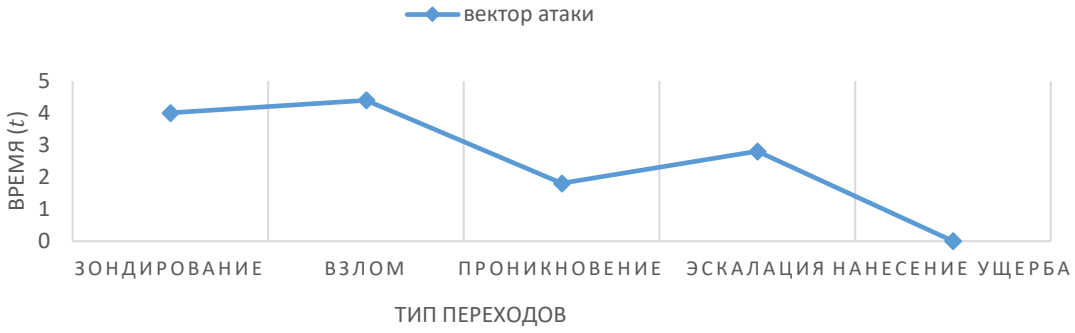

Рис. 4. Пример вектора атаки по числу типов переходов в графе компрометации

Рис. 5. Пример вектора атаки по числу типов тактик

2. Второй тип с учётом топологии сети. Для второго случая предлагается система координат, в которой учитывается уровень VLAN y_i (уровень агрегации сетевых пакетов и возможность воздействия на целевые сетевые узлы), последовательно связанные сетевые узлы (h_i), время фиксации признака угрозы (t_i). Принципы формирования координатной плоскости могут быть разными, предлагаются по степени приближения к ядру инфраструктуры и посегментно.

Для каждой из координат можно записать модель:

$$\begin{cases} y_i = y_{i-1} + \xi_{yi} \\ h_i = h_{i-1} + \xi_{hi} \\ t_i = t_{i-1} + \xi_{ti} \end{cases}. \quad (7)$$

Далее можно представить в векторно-матричной форме для первого и второго случая.

Для первого случая:

$$\begin{bmatrix} y_i \\ t_i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y_{i-1} \\ t_{i-1} \end{bmatrix} \begin{bmatrix} \xi_{hi} \\ \xi_{xi} \end{bmatrix}. \quad (8)$$

Для второго случая:

$$\begin{bmatrix} y_i \\ h_i \\ t_i \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} y_{i-1} \\ h_{i-1} \\ t_{i-1} \end{bmatrix} \begin{bmatrix} \xi_{hi} \\ \xi_{xi} \\ \xi_{xi} \end{bmatrix}. \quad (9)$$

Тогда изменения координат в векторе атаки, а следовательно, и его направление в топологии сети, динамика изменения состояний систем (g_{yi}) по матрице определяются следующим образом (применяется для вычисления каждой координаты):

$$\begin{cases} y_i = y_{i-1} + \xi_{hi} \\ g_{yi} = g_{yi-1} + \xi_{xi} \end{cases}. \quad (10)$$

Наиболее приоритетный вектор будет определяться высокой скоростью достижения цели, то есть наименьшим количеством времени, затраченным на преодоления всех вершин графа конкретной атаки (атаки, характеризуемой связанным набором признаков, комбинацией признаков как маркеров состояний компрометации), и, соответственно, общим количеством времени, затраченным на реализацию вектора атаки.

4. Заключение

Таким образом, при определении вектора атаки в дополнение к методикам, изложенным в методических документах ФСТЭК, а также к теории применения графа компрометации можно использовать векторные марковские последовательности. Их применение представлено в двух подходах, один из которых позволяет рассматривать в двумерном представлении переходы между состояниями компрометации с прогнозированием этих переходов (это дает возможность определить степень достижения цели злоумышленником посредством фиксации актуального состояния компрометации в одной из типовых зон), а второй подход позволяет рассмотреть переходы между компрометируемыми узлами или состояниями этих узлов (также с возможностью прогнозирования последующих состояний). При этом учитывается специфика перемещения фиксации актуальных действий нарушителя внутри или между различными зонами, сегментами сети. Применение одного из приведенных способов рассмотрения вектора атаки позволяет с большей точностью формировать сценарии атаки при анализе угроз информационной безопасности сетевой инфраструктуры. Совмещение этих подходов в дальнейшем предполагает рассмотрение кортежа нескольких разнотипных признаков (в *n*-мерном пространстве), что затруднит визуализацию результатов, но позволить более точно прогнозировать степень повышения опасности при реализации сценария атаки.

Литература

1. Методика оценки угроз безопасности информации // Методический документ ФСТЭК России: утв. ФСТЭК России 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.
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.* Многоагентные технологии анализа уязвимостей и обнаружения вторжений в компьютерных сетях // Новости искусственного интеллекта. 2004. № 1. С. 56–72.
5. *Щеглов А. Ю.* Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и Техника, 2004. 384 с.
6. *Галатенко В. А.* Управление рисками: обзор употребительных подходов (часть 2) // Jet Info. 2018. № 12.
7. *Астахов А.* Введение в аудит информационной безопасности // GlobalTrust Solutions [Электронный ресурс]. 2018. URL: `http://globaltrust.ru` (дата обращения: 29.01.2018).
8. *Аверченков В. И., Рытов М. Ю., Гайнулин Т. Р* Оптимизация выбора состава средств инженерно-технической защиты информации на основе модели Клементса–Хоффмана // Вестник Брянского государственного технического университета. 2008. № 1 (17).

9. Марковские процессы в дискретном времени: [сайт]. URL: https://propproprogs.ru/dsp/markovskie-processy-v-diskretnom-vremeni.

Статья поступила в редакцию 15.05.2022.

Ветров Игорь Анатольевич
к.т.н., доцент, образовательно-научный кластер «Институт высоких технологий», Балтийский федеральный университет им. И. Канта (236041, Калининград, ул. Александра Невского, 14), e-mail: vetrov.gosha2009@yandex.ru.

Подтопельный Владислав Владимирович
старший преподаватель, Институт цифровых технологий ФГБОУ ВО «КГТУ» (236022, Калининград, Советский пр., 1), e-mail: ionpvv@mail.ru.

Vector formation features of modern network attacks

Vetrov Igor Anatolyevich
Candidate of Technical Sciences, Associate Professor, Institute of Physical and Mathematical Sciences and Information Technologies, I. Kant Baltic Federal University (14 Alexander Nevsky Str., Kaliningrad, 236041), vetrov.gosha2009@yandex.ru.

Podtopelny Vladislav Vladimirovich
senior lecturer, Institute of Digital Technologies of KSTU (236022, Sovetsky ave., 1, Kaliningrad, Kaliningrad region), ionpvv@mail.ru.

The problems that arise when setting tasks for determining the vector of a network attack in a corporate information network are considered. The varieties of various techniques that simplify the construction of a network attack vector used in the analysis of the reliability of information systems are presented and characterized. The suitability for various procedures for determining vector parameters is considered. When constructing a network attack vector, the specificity of the manifestation of the time parameter was determined as a characteristic indicating a more effective way of spreading compromise. The formation of the vector is considered taking into account the specifics of the networks multilevel organization. The specifics of the simplified vector calculation model including procedures focused on various approaches are determined.

Keywords: vectors of network attack, information systems, corporate information network, vulnerability.

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. Mnogoagentnye tekhnologii analiza uyazvimostei i obnaruzheniya vtorzhenii v komp'yuternykh setyakh [Multi-agent technologies for vulnerability analysis and intrusion detection in computer networks]. *Novosti iskusstvennogo intellekta*, 2004, no. 1, pp. 56–72.
5. Shcheglov A.Yu. *Zashchita komp'yuternoi informatsii ot nesanktsionirovannogo dostupa* [Protection of computer information from unauthorized access]. Saint Petersburg, Science and Technology, 2004, 384 p.
6. 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-podkhodov-chast-2/` (accessed: 29.01.2022).
7. Astakhov A. Vvedenie v audit informatsionnoi bezopasnosti [Introduction to information security audit [Report]], *GlobalTrust Solutions*, 2018, available at: `http://globaltrust.ru` (accessed: 29.01.2018).
8. Averchenkov V.I., Rytov M.Yu., Gainulin T.R Optimizatsiya vybora sostava sredstv inzhenerno-tekhnicheskoi zashchity informatsii na osnove modeli Klementsa–Khoffmana [Optimization of the choice of the composition of the means of engineering and technical protection of information based on the Clements–Hoffman model]. *Vestnik Bryanskogo gosudarstvennogo tekhnicheskogo universiteta*, Bryansk, 2008, no. 1(17).
9. *Markovskie protsessy v diskretnom vremeni* [Markov processes in discrete time], available at: `https://proproprogs.ru/dsp/markovskie-processy-v-diskretnom-vremeni` (accessed: 29.01.2022).