НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2023 Том 23 № 3 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2023 Vol. 23 No 3 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

doi: 10.17586/2226-1494-2023-23-3-530-537
УДК 004.056

Критерий безопасности сетевой инфраструктуры

Анастасия Дмитриевна Шилова✉

Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
bondareva.ad@yandex.ru✉, https://orcid.org/0000-0001-7271-8343

Аннотация

Введение. Рассмотрена задача оценки безопасности сетевой инфраструктуры. Разработаны и формализованы быстро вычислимые метрики безопасности сети. Метрики предназначены для оценки уровня информационной безопасности сети и применимы для использования в оптимизационных задачах, направленных на перестроение сети по требованиям безопасности. **Метод.** Разработано три метрики безопасности с различной степенью детализации. Сформирован набор важных параметров сетевой инфраструктуры, которые важны для каждого узла с точки зрения продвижения по сети. Набор параметров учитывает актуальные методы бокового перемещения (lateral movement), формализованные в матрице MITRE ATT&CK. Степень детализации метрики позволила учесть наличие в сети терминального доступа, а также фактическую структуру сетевого пути от субъекта к объекту доступа. **Основные результаты.** Произведено сопоставление результатов предложенной базовой метрики с аналогичными метриками других авторов. Показано, что метрика чувствительна к изменениям существенных параметров сети, а результаты ее вычисления согласуются с результатами вычисления других метрик. Выполнена оценка предложенного метода сегментации сети, основанного на группировке субъектов и объектов. Метод позволил значительно повысить защищенность сети за счет объединения схожих субъектов и объектов в группы даже при отсутствии правил межсетевого экранирования. **Обсуждение.** Предложенные метрики могут быть использованы в качестве основы для методов сегментации сетевой инфраструктуры и перестроения существующей сети по требованиям безопасности. При этом они не зависят от параметров, для которых необходима субъективная оценка, а также не учитывают наличие известных уязвимостей, закрытие которых влияет на безопасность в целом, но не отражает защищенность сетевого взаимодействия. Наиболее существенным преимуществом можно считать значительно более быстрое вычисление по сравнению с аналогами.

Ключевые слова

информационная безопасность, сетевая инфраструктура, критерий безопасности, субъект доступа, объект доступа, сегментация сети

Ссылка для цитирования: Шилова А.Д. Критерий безопасности сетевой инфраструктуры // Научно-технический вестник информационных технологий, механики и оптики. 2023. Т. 23, № 3. С. 530–537. doi: 10.17586/2226-1494-2023-23-3-530-537

Criterion of the network infrastructure security

Anastasia D. Shilova✉

ITMO University, Saint Petersburg, 197101, Russian Federation
bondareva.ad@yandex.ru✉, https://orcid.org/0000-0001-7271-8343

Abstract

The problem of assessing the security of a network infrastructure is considered. The aim of the work is to formalize a fast computable network security metric intended for use in optimization problems aimed at rebuilding the network according to security requirements. Three metrics with varying degrees of detail are proposed to achieve this goal. To do this, a set of essential features of the network infrastructure has been formed. The level of detail of the metric allows taking into account the terminal access as well as the actual structure of the network path from the subject to the accessobject. The

proposed base metric was compared with previously published metrics by other authors. It is shown that the metric is sensitive to changes in essential network parameters, and the results of its calculation are consistent with the results of calculation of other metrics. Using the metric, the network segmentation method based on the grouping of subjects and objects was evaluated. It is shown that this method can significantly increase the security of the network by combining similar subjects and objects into groups even in the absence of firewall rules. The proposed metrics can be used as a basis for methods of segmenting the network infrastructure and rebuilding the existing network according to security requirements. They do not depend on a subjective assessment, and also do not take into account the presence of known vulnerabilities the closing of which affect security in general, but does not reflect the security of the network interaction. The most significant advantage can be considered as much faster calculation in comparison with analogues.

Keywords
information security, network infrastructure, security criterion, access subject, access object, network segmentation

For citation: Shilova A.D. Criterion of the network infrastructure security. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2023, vol. 23, no. 3, pp. 530–537 (in Russian). doi: 10.17586/2226-1494-2023-23-3-530-537

Введение

Оценка безопасности сетевой инфраструктуры давно исследуется в научных работах. В настоящее время используется множество метрик, имеющих собственные достоинства и недостатки, тем не менее не существует единого подхода к определению безопасности сетевой инфраструктуры. Большинство существующих методов определения защищенности сети основаны на моделировании деятельности атакующих и построении графов сетевых атак. В связи с этим оценка защищенности информационных систем осуществляется с использованием многоэтапных алгоритмов, требующих значительных трудозатрат.

Несмотря на теоретическую возможность использования метрик безопасности для принятия решения о внедрении защитных механизмов, на практике решения чаще всего принимаются исходя из опыта администраторов безопасности. Это связано с тем, что данные метрики достаточно сложны. Часто дорогостоящие защитные средства внедряются, даже если значительное повышение безопасности возможно с использованием штатных средств.

Цель работы — решение проблемы количественной оценки безопасности сетевой инфраструктуры. Для решения проблемы необходимо сформулировать критерий безопасности сетевой инфраструктуры, на основании которого может быть произведено сопоставление защищенности различных сетей и разработать метрики безопасности сетевой инфраструктуры, предназначенные для решения оптимизационной задачи минимизации рисков в сети. Разработанные метрики должны не только учитывать критичность информационных ресурсов и возможности атакующего, но и быть простыми и быстро вычислимыми для возможности применения в качестве минимизируемой функции в задаче оптимизации.

Анализ предметной области

В работах [1–8] рассмотрена проблема определения уровня защищенности сетевой инфраструктуры. В [2] исследован метод оценки безопасности сети с использованием графа атак. При вычислении метрик применены таблицы, подобные используемым в методиках, утверждаемых Федеральной службой по техническому и экспортному контролю (ФСТЭК)[1]. Отметим, что применение метода оценки можно считать одним из недостатков, так как он не учитывает специфику функционирования информационных систем. В работе [3] метод оценки был усовершенствован за счет использования метрик Common Vulnerability Scoring System (CVSS). В отличие от [2] данный подход не подразумевает использование упрощенных табличных оценок и в большей степени отражает особенности функционирования сетевой инфраструктуры. Схожий метод оценки защищенности исследован в работе [4]. Он основан на определении слабости хостов к потенциальным атакам. При этом учитываются только критичные уязвимости со значением Common Weakness Scoring System (CWSS) более 60, что не позволяет полноценно оценить защищенность от полного спектра атак.

В [4] представлена методика оценки рисков, основанная на полученных в [2, 3] результатах. Метрика модифицирована для оценки риска и составлена с помощью модели действий злоумышленника, основанная на графах. Метрика зависит от экспертного подхода: например, вероятность атаки зависит от сложности, что часто не может быть оценено объективно. Также не учтены некоторые факторы, влияющие на безопасность сети, в частности наличие прав локального администратора или ошибки пользователей. В работах [7–9] произведено построение графа действий атакующих. Отличительной особенностью подхода является использование вероятностного описания для каждого ребра, что позволяет вычислить вероятностную оценку безопасности сети.

В описанных работах осуществлено построение графа возможных действий злоумышленника. Создание исчерпывающего графа и сбор данных представляют собой трудноразрешимую задачу. По этой причине большинство алгоритмов не учитывает существенную часть атак. Кроме того, построение графа и расчет метрик безопасности требуют значимых затрат времени и ресурсов. Математическая оптимизация таких метрик не представляется возможной. Отметим, что данные методы в большинстве случаев используют метрики CVSS, в которых присутствуют субъективно настраи-

[1] Методика оценки угроз безопасности информации. Методический документ. Утвержден ФСТЭК России, 5 февраля 2021 г.

ваемые параметры, а ценность активов определяется ранжированием по ограниченному числу уровней. Еще одной особенностью данных работ может считаться то, что в них учитываются заведомо осуществимые атаки. При построении же защищенной сети отсутствие устаревшего программного обеспечения (ПО) или заведомо некорректных настроек должно являться обязательным условием.

Обзор альтернативных метрик защищенности сетевой инфраструктуры приведен в работе [6], где проведено разделение метрик, предназначенных для контроля безопасности узла и безопасности сети, учитывающие и не учитывающие путь проникновения в сеть. Недостатком метрик, не учитывающих порядок действий злоумышленников, является их нацеленность на защищенность узлов: безопасность сети рассмотрена как доля уязвимых узлов.

Заметим, что все рассмотренные работы не учитывают уязвимости нулевого дня и уязвимости, связанные с ошибками в работе персонала. Отсутствие логической сетевой связности между сегментами сети позволяет значительно снизить вероятность компрометации даже при использовании подобных уязвимостей.

Модель сетевой инфраструктуры

Для построения метрики оценки безопасности сети необходимо представить математическое описание (модель) сетевого взаимодействия. В качестве основы для его построения рассмотрим ориентированный граф сетевых взаимодействий, в узлах которого расположены используемые маршрутизаторы и конечные устройства. Субъектами взаимодействия будем считать пользовательские устройства (автоматизированные рабочие места), а объектами — вычислительные устройства, на которых размещены применяемые информационные системы, доступные посредством сетевых протоколов.

Основой модели служит понятие пути. Каждому ребру соответствует матрица, состоящая из переменных, отражающих запрещающие правила межсетевого экранирования на узле, расположенном в начале ребра:

$$\mathbf{X}^{(\mathbf{r})} = ||x_{ij}^{(r)}||,$$

где x_{ij} — переменная, принимающая значение 0 или 1 и отражающая запрещающее правило для соответствующих субъекта и объекта. Путь от каждого субъекта S_i до каждого объекта O_j представляет собой последовательность ребер ориентированного графа.

Наличие пути выразим соотношением:

$$P_{ij} = \prod_{r \in P} (1 - x_{ij}^{(r)}),$$

где P — множество ребер в пути от субъекта S_i до объекта O_j. Отметим, что полученная модель не накладывает ограничений на количество путей от субъекта до объекта. При этом, если в сети существует несколько путей между субъектом и объектом доступа (при использовании балансировки трафика или протоколов, осуществляющих перестроение таблиц маршрутизации), то получим следующие обобщение сети:

$$P_{ij} = 1 - \prod_{n} P_{ij}^{(n)},$$

где $P_{ij}^{(n)}$ — частный путь от субъекта до объекта.

Полученная модель предназначена, в первую очередь, для определения возможности получения доступа субъекта к объекту. Рассмотрим метрики, основанные на матрице MITRE ATT&CK и включающие в себя важные характеристики с точки зрения продвижения по сети и атаки на информационные системы. В качестве угрозы в данной модели рассмотрим несанкционированный доступ любого рода со стороны субъекта к объекту на сетевом уровне. Поставим условие, что разрабатываемые метрики должны отражать повышение защищенности при устранении избыточных путей, которые могут быть использованы потенциальными злоумышленниками.

Предлагаемые метрики

Предложенная метрика основана на модели сетевой инфраструктуры. Под критичностью каждого пути будем понимать величину, зависящую от уровня возможностей потенциального атакующего, значимости обрабатываемой информации, возможности использования объекта для продвижения по сети, а также от применяемых средств защиты. Данные характеристики в значительной степени заимствованы из матрицы MITRE ATT&CK, отражающей современные процедуры, тактики и техники, применяемые злоумышленниками.

Отметим, что рассматриваемые далее метрики аналогичны общепризнанному методу вычисления уровня риска с единственным отличием, что введен формальный механизм вычисления вероятности реализации угрозы.

Обобщенная метрика безопасности. Для каждого субъекта определим набор характеристик, существенных с точки зрения проведения субъектом атак на сетевую инфраструктуру. Пусть Y_i — уровень возможностей субъекта S_i. Данная величина является порядковой и принимает следующие значения: 1 — обычные пользовательские привилегии, 2 — наличие средств администрирования, 3 — наличие средств разработки, 4 — права локального администратора, 5 — права доменного администратора. С точки зрения атак на информационную инфраструктуру данные уровни отражают возможности, которыми обладает потенциальный злоумышленник для проведения атак на информационные ресурсы, бокового перемещения и доставки инструментов для выполнения несанкционированных действий. Данная величина определена по аналогии с установлением уровня возможностей нарушителя информационной безопасности, используемыми в различных методиках и моделях угроз ФСТЭК[1,2].

[1] Методика оценки угроз безопасности информации. Методический документ. Утвержден ФСТЭК России, 5 февраля 2021 г.

[2] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утвержден ФСТЭК России, 15 февраля 2008 г.

Пусть Z_i — величина, которая отражает наличие средств защиты субъекта (на вычислительном устройстве) и принимает значение 0 или 1. В различных организациях могут использоваться различные механизмы противодействия угрозам, например, подключение к системам мониторинга Security Operations Center (SOC) или средства обнаружения целевых атак, имеющим в зависимости от контекста и условий применения различную эффективность. Тем не менее, любые средства защиты затрудняют продвижение по сети и осуществление атак в соответствии с тактиками и техниками.

Пусть I_i — величина, которая отражает наличие доступа субъекта в сеть Интернет и приобретает значения 0 и 1. С точки зрения тактик и техник данная характеристика важна, поскольку упрощает доставку инструментария для проведения атак.

Определим характеристики объекта. Пусть L_j — значимость машины с точки зрения продвижения по сети. Возможность использования сервиса для дальнейшего продвижения по сети и атак на другие сервисы должна быть учтена при оценке безопасности сети. Порядок действий при компрометации информационной инфраструктуры формализуем в форме так называемых cyberkillchain (CKC) [10], которые в дальнейшем расширим до полноценной матрицы — ATT&CK, разработанной MITRE. На ее основе определим возможные сценарии использования устройств, поддерживающих следующие сервисы:

1) наличие средства удаленного управления (Lateral Movment: Remote Services);
2) наличие доступных для машины подсетей (Lateral Movement: Exploitation of Remote Services, Privilege Escalation: Escape to Host);
3) наличие машин, управляемых с использованием данной машины (Privilege Escalation: Escape to Host; Lateral Movement: Software Deployment Tools);
4) наличие учетной записи с возможностью делегирования (Credential Access: Steal of Forge of Kerberos Tickets; Privilege Escalation: Access Token Manipulation);
5) необходимость периодического создания сессии учетной записи с высокими привилегиями (Lateral Movement: Use Alternate Authentication Material);
6) наличие сохраненных паролей (Credential Access: Credentials from Password Stores);
7) наличие общих хранилищ (Lateral Movement: Taint Shared Content);
8) наличие сведений о структуре сети (Discovery).

Поскольку структура сети при ее перестроении может изменяться, параметр значимости L_j вычислим, исходя из наихудшего варианта развития событий. В перспективе данный параметр может быть заменен на число атакующих «трасс» [2, 11], однако для этого требуются более быстрые методы вычисления по сравнению с существующими.

Величина V_j отражает степень критичности активов. Предположим, что это неотрицательное число, полученное путем порядковой оценки критичности активов. Величина W_j принимает значение 0 или 1 и отражает наличие средств защиты объекта. Ее назначение совпадает с аналогичной величиной для субъекта. Величина G_j отражает источник ПО. Она принимает следующие значения: 1 — собственная разработка, 2 — приложение с открытым кодом, 3 — коммерческое приложение. Величина G_j введена в соответствии с предположением, что приложения собственной разработки в большинстве организаций не проходят процедуру верификации и поиска уязвимостей, тогда как для приложений с открытым исходным кодом осуществляется поиск уязвимостей свободными исследователями. Коммерческое приложение, используемое в организациях, чаще проходит процедуру сертификации, тестируется отделами безопасности, а также исследуется в рамках программ поиска уязвимостей и при тестированиях на проникновение, потому в них менее вероятно наличие критических уязвимостей.

Определим общую критичность пути от субъекта до объекта:

$$C_{ij} = V_j\left(\frac{3+Y_i}{8}\right)\left(\frac{8+L_j}{16}\right)\left(1-\frac{W_j}{2}\right)\left(1-\frac{Z_i}{2}\right)\times \times\left(\frac{5-G_j}{4}\right)\left(\frac{1+I_i}{2}\right) \quad (1)$$

Формула (1) представляет собой мультипликативный критерий, который формируется за счет умножения отдельных характеристик объекта. Коэффициенты для характеристик выбраны таким образом, чтобы в наиболее благоприятной ситуации соответствующий множитель был равен 0,5, а в наименее благоприятной — 1. Данные значения выбраны, исходя из ограничений модели и решаемой задачи: наиболее благоприятная ситуация не исключает угрозу, однако снижает вероятность ее реализации. Фактически формула (1) подобна формуле вычисления риска [12], в которой вероятность атаки заменена на эквивалентную величину, отражающую возможности потенциального атакующего и степень защищенности объекта.

Получим расчет аддитивного критерия безопасности:

$$R = \sum_{i=1}^{N_O}\sum_{j=1}^{N_S} C_{ij}P_{ij},$$

где N_O и N_S — числа объектов и субъектов.

Метрика с учетом терминального доступа. Рассмотрим подход, при котором в инфраструктуре организации присутствуют терминалы (T_t), которые используются при организации доступа к изолированным сетевым сегментам. При наличии в пути терминалов рассматривается не только исходная машина, но и последний в пути терминал. Все пути могут быть разделены на несколько групп: путь от терминала к объекту, путь от субъекта к терминалу, путь от субъекта к объекту. Для каждого терминала характерно множество пользователей (субъектов), для каждого из которых характерен уровень возможностей $Y_i^{(T)}$. Уровень возможностей терминала может отличаться от уровня возможностей на используемом субъектом устройстве (вследствие наличия средств защиты и мониторинга на границе сети). Аналогично для терминала могут использоваться средства защиты, что определяет величину $Z_i^{(T)}$.

Критичность пути от пользователя терминала к объекту имеет вид:

$$C_{ij} = V_j\left(\frac{3+Y_i^{(T)}}{8}\right)\left(\frac{8+L_j^{(T)}}{16}\right)\left(1-\frac{W_j}{2}\right)\times \times\left(1-\frac{Z_i^{(T)}}{2}\right)\left(\frac{5-G_j}{4}\right)\left(\frac{1+I_i}{2}\right) \quad (2)$$

Вычислим аддитивный критерий безопасности:

$$R = \sum_{i=1}^{N_O}\sum_{j=1}^{N_S} C_{ij}P_{ij} + \sum_{i=1}^{N_O}\sum_{j=1}^{N_S}\sum_{t=1}^{N_T} P_{it}P_{tj}C_{tj},$$

где N_T — число терминалов.

Достоинствами метрик являются скорость вычисления (параметры для пар могут быть вычислены заранее), возможность оптимизации (функция дифференцируема) и учет структуры сети. При этом присутствует одна (условно) экспертная метрика — критичность. Основной недостаток метрики — большое число параметров, что усложняет задачу оптимизации.

Анализ предложенных подходов

Перечисленные метрики являются частными случаями обобщенной метрики. Для оценки ее применимости при определении степени защищенности сети продемонстрируем ее достаточность и реакцию на изменения сети.

Синтетический пример. Для оценки реакции на изменение сети рассмотрим варианты сети из 7 узлов с различными конфигурациями и применяемыми мерами защиты (рисунок). Во всех сетях используем идентичные субъекты S и объекты O. Для субъектов и объектов установим следующие характеристики (табл. 1).

В табл. 2 представлены результаты оценки безопасности исследованных сетей.

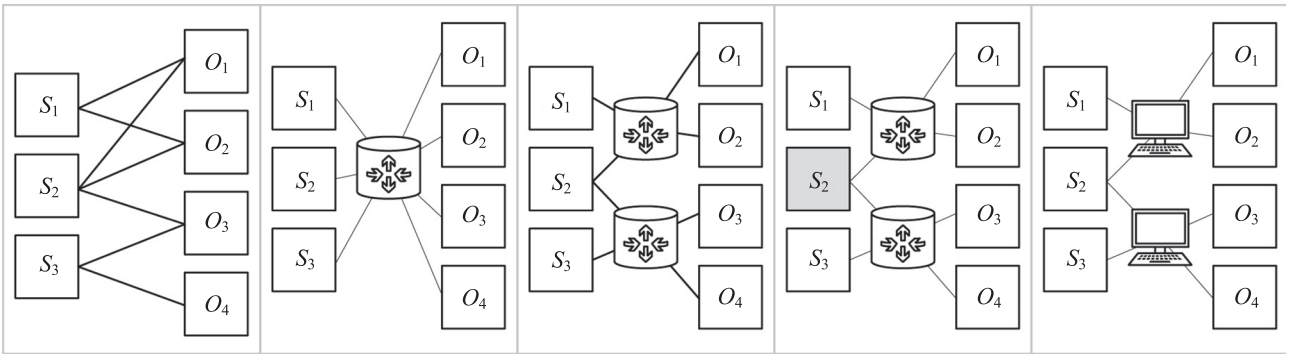

Рисунок. Сопоставляемые сети: эталон (*a*); связь «все со всеми» (*b*); сегментация (*c*); сегментация + мониторинг (*d*); терминальный доступ (*e*)

Figure. Comparable networks: optimal (*a*); connection “all to all” (*b*); segmentation (*c*); segmentation + monitoring (*d*); terminal access (*e*)

Таблица 1. Характеристики субъектов и объектов

Table 1. Characteristics of subjects and objects

Субъект	Параметры	Объект	Параметры	Терминал	Параметры
S_1	Y: 1, Z: 0, I: 0	O_1	L: 4, V: 1, W: 0, G: 3	T_1 (S_1)	Y: 1
S_2	Y: 2, Z: 0, I: 0	O_2	L: 3, V: 2, W: 0, G: 1	T_1 (S_2)	Y: 1
S_3	Y: 3, Z: 0, I: 0	O_3	L: 5, V: 3, W: 1, G: 2	T_2 (S_2)	Y: 2
S_2 + SOC	Y: 2, Z: 1, I: 0	O_4	L: 2, V: 4, W: 1, G: 1	T_3 (S_2)	Y: 1

Таблица 2. Метрики безопасности для сопоставляемых сетей

Table 2. Security metrics for compared networks

Сеть	Структура сети	Метрика безопасности
эталон	целевая реализация — каждый пользователь (субъект) имеет доступ только к подмножеству объектов, необходимых для работы	2,082
связь «все со всеми»	плоский вариант — все субъекты имеют сетевой доступ ко всем объектам	3,669
сегментация	сегментация с использованием двух узлов маршрутизации — эквивалентна одному роутеру с правилами разграничения доступа	2,472
сегментация + мониторинг	сегментация с использованием двух узлов маршрутизации — наличие настроенных средств мониторинга на компьютере S2	1,861
терминальный доступ	использование двух терминалов	2,092

Наименьшее значение метрики безопасности достигнуто при использовании терминалов (сеть «терминальный доступ») или мониторинга силами SOC (сеть «сегментация + мониторинг»), что согласуется с установленными во многих организациях правилами работы. При этом снижение количества избыточных связей или увеличение количества мер защиты влечет изменение предложенной метрики. На практике защитные механизмы при осуществлении сегментации могут не учитываться, благодаря чему формула (2) значительно упрощается:

$$C_{ij} = V_j\left(\frac{3 + Y_i}{8}\right)\left(\frac{8 + L_j}{16}\right).$$

Сопоставление с аналогами. До настоящего времени наборы данных для сегментации сети не были собраны (за редким исключением[1]). Для оценки достаточности предложенной метрики допустимо рассмотреть ее согласованность с ранее предложенными подходами к анализу безопасности сетей. Во многих случаях прямое сопоставление результатов не представляется возможным, поскольку во многих работах: исходная информация — граф атак, а не сетевая топология; в качестве исходных данных используется перечень устаревшего ПО, а план мероприятий сводится к его обновлению (в результате сетевая топология фактически не изменяется); используются неприменимые к предлагаемой параметры, например, сложность атаки или исходная квалификация злоумышленника.

В работе [2] рассмотрен подход, основанный на качественных метриках защищенности. Предложенный в [6] метод нацелен на приоритезацию устранения уязвимостей. При этом учитывается не только критичность, но и требуемые на внедрение средства. В [13, 14] анализ безопасности осуществляется как для сетевой топологии, так и для ее поведения в условиях различных атак. В соответствии с предложенной метрикой была рассчитана величина метрики при устранении одной из связей. Рассмотрим результаты данных подходов в сопоставлении с метрикой, разработанной в настоящей работе (табл. 3).

[1] Dataset for research on services and users grouping [Электронный ресурс]. Режим доступа: https://github.com/ Shtrikh17/datasets, свободный, (дата обращения: 27.05.2022).

Таким образом, созданная метрика реагирует на изменения топологии сети, согласуется с результатами, полученными в других работах, и отражает повышение защищенности при уменьшении поверхности атаки. В сравнении с аналогами она включает в себя меньше параметров и может быть оптимизирована. Отметим, что метрика не учитывает реакцию на защиту от конкретных типов атак (например, перебора паролей ssh), поэтому для точной оценки рисков должны применяться другие метрики, например, рассмотренные в разделе «Предлагаемые метрики».

Метод группировки субъектов и объектов

Рассмотрим работу метрики для рассмотренного в [15] метода группировки субъектов и объектов. Одним из его применений может быть сегментация: все рабочие станции и серверные приложения разделяются на подсети, между которыми разграничивается доступ. Тогда снижается количество рассматриваемых сущностей.

Для рассмотренного в разделе «Анализ предложенных подходов» набора данных реальной организации создана матрица доступа «субъекты-объекты». В соответствии с этими данными осуществлен расчет метрики защищенности для эталонной (рисунок, *a*), плоской (рисунок, *b*) и сегментированной (рисунок, *c*) сетей. При этом в качестве параметров субъектов (объектов) рассмотрены максимальные параметры для каждого субъекта (объекта) в выделенной группе. В результате получены следующие значения метрики для сетей: исходной — 2545,913; идеальной — 629,276 и сегментированной — 1670,479.

Следовательно, предложенный в [15] метод может быть использован для первичной сегментации сети. Дальнейшее повышение безопасности сетевого взаимодействия должно осуществляться с использованием правил межсетевого экранирования.

Обсуждение результатов

Достоинствами предложенной метрики можно считать.

1. Предположение о гарантированном наличии уязвимостей в ПО. При формировании метрики не делается предположений о вероятности их наличия.

Таблица 3. Сравнение результатов аналогичных подходов и предложенной метрики
Table 3. Comparison of the results of similar approaches and the proposed metric

Аналогичные подходы			Предложенная метрика
Ссылка на аналогичную работу	Принцип сети	Используемая метрика	
[2] (качественная величина)	Пример 1	SecurityLevel=Red	3,996
	Пример 2	SecurityLevel=Yellow	3,586
[6] (больше — лучше)	До внедрения защитных мер	622	2,857
	После внедрения защитных мер	2571,9	2,174
[14] (меньше — лучше)	Сеть до запрета соединения с частью узлов	5,637	0,531
	Сеть после запрета соединения с частью узлов	4,581	0,350

2. Использование в качестве входных данных простых величин, выраженных в порядковых шкалах. Построение исчерпывающего графа атак представляется крайне трудоемкой задачей по аудиту, которую практически невозможно провести в кратчайшие сроки.
3. Использование тактик и техник, выделенных в MITRE ATT&CK. В результате повышается скорость вычисления характеристики, снижается сложность ее оценки, а также учитывается возможность использования устройства в качестве промежуточного звена атаки.
4. Возможность оптимизации и скорость вычисления.

Однако у метрики есть несколько недостатков, которые необходимо учитывать при ее выборе для анализа безопасности сети.

1. В отличие от альтернативных подходов данная метрика не учитывает возможность проведения цепочек атак, когда скомпрометированные машины используются в качестве промежуточных звеньев при атаке на другие элементы инфраструктуры.
2. В отличие от данной метрики многие альтернативные метрики позволяют построить цепочку мероприятий, направленных на снижение рисков.

Первый недостаток может быть устранен, если рассмотреть объекты одновременно в качестве субъектов. Однако при этом необходимо дополнительно решить проблему циклов в полученном графе. Кроме того, в перспективе цепочки атак могут использоваться в качестве замены для параметра значимости узла при продвижении по сети. Второй недостаток может быть скорректирован за счет применения других метрик, заимствующих механизмы в аналогичных работах.

Заключение

В работе предложена метрика оценки защищенности сетевой инфраструктуры от потенциальных атак. Она может быть использована в качестве основы для критерия безопасности при построении (перестроении) сетевой инфраструктуры. Оценка данной метрики показывает ее чувствительность к изменению параметров, а также демонстрирует согласованность с результатами, полученными другими исследователями. Выполнено сопоставление с существующими аналогами, предназначенными для оценки защищенности сети. В качестве примера использования данного критерия рассмотрен подход к сегментации на основе группировки субъектов и объектов сетевого доступа [15].

Целью дальнейших исследований является модификация метрики для учета цепочек атак, а также ее практическое применение для перестроения сетевой инфраструктуры с использованием теории графов и методов оптимизации. При этом возможно ее дальнейшее расширение для учета более сложных атак, зависящих от сетевой топологии, но на данный момент не использованных при построении метрики.

Литература

1. Li G., Fu Y., Hao W. Quantifiable network security measurement: A study based on an index system // Lecture Notes in Computer Science. 2019. V. 11806. P. 47–62. https://doi.org/10.1007/978-3-030-30619-9_5
2. Котенко И.В., Степашкин М.В., Богданов В.С. Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности // Труды СПИИРАН. 2006. Т. 2. N 3. С. 30–49. https://doi.org/10.15622/sp.3.2
3. Дойникова Е.В., Чечулин А.А., Котенко И.В. Оценка защищенности компьютерных сетей на основе метрик CVSS // Информационно-управляющие системы. 2017. № 6(91). С. 76–87. https://doi.org/10.15217/issn1684-8853.2017.6.76
4. Шинкаренко А.Ф. Методика оценивания защищенности информационно-телекоммуникационных узлов // Интеллектуальные технологии на транспорте. 2016. № 1(5). С. 16-19 [Электронный ресурс]. URL: http://itt-pgups.ru/index.php/itt_pgups/article/view/3322, свободный. Яз. рус. (дата обращения: 12.06.2022).
5. Дойникова Е.В., Котенко И.В. Методики и программный компонент оценки рисков на основе графов атак для систем управления информацией и событиями безопасности // Информационно-управляющие системы. 2016. № 5(84). С. 54–65. https://doi.org/10.15217/issn1684-8853.2016.5.54
6. Poolsappasit N., Dewri R., Ray I. Dynamic security risk management using bayesian attack graphs // IEEE Transactions on Dependable and Secure Computing. 2012. V. 9. N 1. P. 61–74. https://doi.org/10.1109/TDSC.2011.34
7. Dantu R., Kolan P. Risk management using behavior based bayesian networks // Lecture Notes in Computer Science. 2005. V. 3495. P. 115–126. https://doi.org/10.1007/11427995_10
8. Котенко И.В., Дойникова Е.В. Методика выбора контрмер в системах управления информацией и событиями безопасности // Информационно-управляющие системы. 2015. № 3(76). С. 60–69. https://doi.org/10.15217/issn1684-8853.2015.3.60

References

1. Li G., Fu Y., Hao W. Quantifiable network security measurement: A study based on an index system. *Lecture Notes in Computer Science*, 2019, vol. 11806, pp. 47–62. https://doi.org/10.1007/978-3-030-30619-9_5
2. Kotenko I.V., Stepashkin M.V., Bogdanov V.S. Evaluating security of computer networks based on attack graphs and qualitative security metrics. *SPIIRAS Proceedings*, 2006, vol. 2, no. 3, pp. 30–49. (in Russian). https://doi.org/10.15622/sp.3.2
3. Doynikova E.V., Chechulin A.A., Kotenko I.V. Computer network security evaluation based on CVSS metrics. *Information and Control Systems*, 2017, no. 6(91), pp. 76–87. (in Russian). https://doi.org/10.15217/issn1684-8853.2017.6.76
4. Shinkarenko A.F. The method of estimation of the security of information and telecommunication. *Intellectual Technologies on Transport*, 2016, no. 1(5), pp. 16–20. Available at: http://itt-pgups.ru/index.php/itt_pgups/article/view/3322 (accessed: 12.06.2022). (in Russian)
5. Doynikova E.V., Kotenko I.V. Techniques and software tool for risk assessment on the base of attack graphs in information and security event management systems. *Information and Control Systems*, 2016, no. 5(84), pp. 54–65. (in Russian). https://doi.org/10.15217/issn1684-8853.2016.5.54
6. Poolsappasit N., Dewri R., Ray I. Dynamic security risk management using bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 2012, vol. 9, no. 1, pp. 61–74. https://doi.org/10.1109/TDSC.2011.34
7. Dantu R., Kolan P. Risk management using behavior based bayesian networks. *Lecture Notes in Computer Science*, 2005, vol. 3495, pp. 115–126. https://doi.org/10.1007/11427995_10
8. Kotenko I.V., Doynikova E.V. Countermeasure selection in security management systems. *Information and Control Systems*, 2015, № 3(76), pp. 60–69. (in Russian). https://doi.org/10.15217/issn1684-8853.2015.3.60

9. Wing J.M. Scenario graphs applied to network security // Information Assurance. Elsevier, 2008. P. 247–277. https://doi.org/10.1016/B978-012373566-9.50011-2
10. Mihai I., Prună S., Barbu I.-D. Cyber kill chain analysis // International Journal of Information Security and Cybercrime. 2014. V. 3. N 2. P. 37–42. https://doi.org/10.19107/IJISC.2014.02.04
11. Lin W., Yang C., Zhang Z., Xue X., Haga R. A quantitative assessment method of network information security vulnerability detection risk based on the meta feature system of network security data // KSII Transactions on Internet and Information Systems. 2021. V. 15. N 12. P. 4531–4544. https://doi.org/10.3837/tiis.2021.12.015
12. Крылова Ю.В. Оценка рисков и угроз информационной безопасности в организации // МСФО в современной экономике России: модели, схемы и способы практической реализации: материалы Международной студенческой научно-практической конференции. М., 2019. С. 142–146.
13. Zhao X., Pei M., Wu M., Liang Y., Peng H. A method of network security risk measurement based on improved D-S evidence theory // Journal of Physics: Conference Series. 2020. V. 1626. P. 012035. https://doi.org/10.1088/1742-6596/1626/1/012035
14. Zhao X., Zhang Y., Xue J., Shan C., Liu Z. Research on network risk evaluation method based on a differential manifold // IEEE Access. 2020. V. 8. P. 66315–66326. https://doi.org/10.1109/ACCESS.2020.2985547
15. Bondareva A., Shilov I. Method of grouping subjects and objects in information systems // Proc. of the 30th Conference of Open Innovations Association FRUCT. 2021. P. 10–15. https://doi.org/10.23919/FRUCT53335.2021.9599989

9. Wing J.M. Scenario graphs applied to network security. *Information Assurance*. Elsevier, 2008, pp. 247–277. https://doi.org/10.1016/B978-012373566-9.50011-2
10. Mihai I., Prună S., Barbu I.-D. Cyber kill chain analysis. *International Journal of Information Security and Cybercrime*, 2014, vol. 3, no. 2, pp. 37–42. https://doi.org/10.19107/IJISC.2014.02.04
11. Lin W., Yang C., Zhang Z., Xue X., Haga R. A quantitative assessment method of network information security vulnerability detection risk based on the meta feature system of network security data. *KSII Transactions on Internet and Information Systems*, 2021, vol. 15, no. 12, pp. 4531–4544. https://doi.org/10.3837/tiis.2021.12.015
12. Krylova Iu.V. Assessment of information security risks and threats in the organization. IRFS in the modern Russian economy: models, schemes and methods of practical implementation. *Proceedings of the International Scientific and Practical Conference of Students*. Moscow, 2019, pp. 142–146. (in Russian)
13. Zhao X., Pei M., Wu M., Liang Y., Peng H. A method of network security risk measurement based on improved D-S evidence theory. *Journal of Physics: Conference Series*, 2020, vol. 1626, pp. 012035. https://doi.org/10.1088/1742-6596/1626/1/012035
14. Zhao X., Zhang Y., Xue J., Shan C., Liu Z. Research on network risk evaluation method based on a differential manifold. *IEEE Access*, 2020, vol. 8, pp. 66315–66326. https://doi.org/10.1109/ACCESS.2020.2985547
15. Bondareva A., Shilov I. Method of grouping subjects and objects in information systems. *Proc. of the 30th Conference of Open Innovations Association FRUCT*, 2021, pp. 10–15. https://doi.org/10.23919/FRUCT53335.2021.9599989

Автор

Шилова Анастасия Дмитриевна — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0000-0001-7271-8343, bondareva.ad@yandex.ru

Author

Anastasia D. Shilova — PhD Student, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0000-0001-7271-8343, bondareva.ad@yandex.ru

Статья поступила в редакцию 10.10.2022
Одобрена после рецензирования 13.02.2023
Принята к печати 16.05.2023

Received 10.10.2022
Approved after reviewing 13.02.2023
Accepted 16.05.2023