РАЗРАБОТКА АЛГОРИТМА подсистемы обнаружения вторжений

Е.Ряполова, канд. пед. наук, доцент кафедры математики и естественно-научных дисциплин Оренбургского филиала ПГУТИ / ananeva_ei@mail.ru,
М.Студянникова, канд. пед. наук, доцент кафедры математики и естественно-научных дисциплин Оренбургского филиала ПГУТИ / studyannikovam@mail.ru

УДК 004.4, DOI: 10.22184/2070-8963.2022.103.3.70.78

В статье освещены вопросы разработки алгоритма и программного средства обнаружения вторжений. Предлагается схема построения статистического признака, в которой в качестве основного компонента для обнаружения неконтролируемых аномалий объединены факторный анализ и кластеризация k-средних.

По мере роста интереса к обнаружению вторжений также привлекает к себе большое внимание тема оценки систем обнаружения вторжений. Такая оценка является сложной задачей по нескольким причинам.

Во-первых, проблематично получить высококачественные данные для проведения оценки из-за вопросов конфиденциальности и конкуренции, поскольку многие компании и организации не хотят делиться своей служебной информацией с другими учреждениями.

Во-вторых, даже если бы реальные данные были доступны, маркировка сетевых подключений как обычных или навязчивых требует затраты огромного количества времени многими специалистами.

В-третьих, постоянное изменение сетевого трафика может не только вводить новые типы вторжений, но и изменять аспекты "нормального" поведения, что еще более затрудняет построение полезных тестов.

Наконец, при измерении производительности систем обнаружения вторжений необходимо измерять не только частоту обнаружения (т. е. сколько атак мы обнаружили правильно), но и частоту ложных тревог (т. е. сколько нормальных соединений мы неверно определили как атаки), а также стоимость ошибочной классификации. Оценка дополнительно усложняется тем фактом, что некоторые из атак (например, отказ в обслуживании (DoS), зондирование) могут использовать сотни сетевых пакетов или соединений, в то время как, с другой стороны, такие атаки, как U2R (пользователь – Root) и R2L (удаленный на локальный), обычно используют только одно или несколько соединений.

Стандартные показатели, которые были разработаны для оценки вторжений в сеть, обычно соответствуют частоте обнаружения, а также частоте ложных тревог (табл.1). Коэффициент обнаружения вычисляется как отношение количества правильно обнаруженных атак к общему количеству

Таблица 1. Стандартные метрики для оценки вторжений (атак) одного соединения

Стандартные метрики		Предсказанная метка подключения	
		Нормальный	Вторжения (атаки)
Фактическая метка подключения	Нормальный	Правдиво отрицательный	Ложная сигнализация
	Вторжения (атаки)	Ложная сигнализация	Верно обнаруженные атаки

атак, в то время как уровень ложных срабатываний вычисляется как отношение количества нормальных соединений, которые неправильно классифицируются как атаки (ложные срабатывания), к общему количеству нормальных соединений [6, 7].

Обычно при обнаружении вторжений в сеть устанавливаются два типа атак: атаки с использованием отдельных соединений и атаки с использованием нескольких соединений (пакеты соединений) [1]. Стандартные метрики одинаково обрабатывают все типы атак, таким образом, не обеспечивая достаточно общую и систематическую оценку атак, которые включают в себя множество сетевых подключений (пакетные атаки). В частности, они не собирают информацию о количестве сетевых подключений, связанных с атакой, которые были правильно обнаружены. Следовательно, в зависимости от типа атаки могут применяться два вида анализа:

- анализ атак с несколькими подключениями для пакетных атак;
- анализ атак с использованием одного подключения для атак с одним подключением [5].

Для разработки системы обнаружения необходимо определить важные входные функции. Авторами предложена схема построения статистического признака, в которой факторный анализ сочетается с оптимизированной техникой кластеризации k-средних. Метод k-средних – это метод кластерного анализа, цель которого является разделение m наблюдений на k кластеров, при этом каждое наблюдение относится к тому кластеру, к центру которого оно ближе всего.

В качестве основного компонента для обнаружения неконтролируемых аномалий предлагаемая схема построения признаков способна оптимально исключить избыточность признаков посредством рассмотрения сходства ответов признаков посредством кластерного анализа, основанного на пространстве признаков, уменьшенном в факторном анализе.

Эффективность оценивается с использованием различных наборов данных, уменьшенных в результате ранжирования важности входных функций. Экспериментальные результаты [3] показывают значительную частоту обнаружения благодаря хорошим подмножествам функций, которые считаются критическими для улучшения производительности классификаторов.

Построение функции на основе имеющихся данных жизненно важно для эффективности используемых методов. Конструкция объекта улучшает классификацию путем поиска подмножества объектов, которое лучше всего классифицирует данные обучения. Кроме того, сокращение объема данных и последующая классификация вторжений на основе уменьшенного пространства признаков имеют важное значение для обнаружения вторжений в режиме реального времени. В наборе данных по обнаружению вторжений данные проникновения распределены в три набора функций:

- основные;
- функции контента;
- функции трафика.

Традиционные системы обнаружения аномалий требуют чистых данных для обучения, чтобы изучить модель нормального поведения. Основным недостатком этих систем является то, что чистые данные для обучения не всегда доступны. Более того, при обучении на основе зашумленных данных эти системы могут научиться воспринимать навязчивое поведение как нормальное. Чтобы преодолеть эту слабость, необходимо чтобы в основе исследования находились алгоритмы обнаружения вторжения, называемые обнаружением аномалий без присмотра (также известны как обнаружение аномалий по шумным данным). Эти алгоритмы принимают в качестве входных набор немаркированных данных, где неизвестно, какие из них являются нормальными элементами и

какие – аномальными. Затем они пытаются выявить вторжения в данные. Обнаружение неконтролируемой аномалии делает актуальными два предположения относительно данных обучения, которые мотивируют общий подход:

- Предположение 1. Количество нормального трафика в обучающих данных больше, чем количество трафика атаки;
- Предположение 2. Трафик атаки статистически отличается от обычного трафика.

Основная идея заключается в том, что, поскольку аномалии отличаются от нормальных активностей и являются редкими, они будут отображаться как выбросы, которые можно обнаружить в данных.

К обучающим данным применяется кластеризация. Поскольку предполагается, что доля нормальных данных в подавляющем большинстве случаев велика, то считается, что все маленькие кластеры содержат аномалии, а большие кластеры – нормальные активности. Сравним эффективность алгоритмов обнаружения неконтролируемых аномалий:

- алгоритм кластеризации с фиксированной шириной;
- оптимизированная версия алгоритма k-ближайшего соседа.

Основное преимущество алгоритма с фиксированной шириной состоит в том, что он масштабируется линейно с количеством объектов в наборе данных и количеством атрибутов объектов. Тем не менее, качество кластеров чувствительно к ширине кластера, и часто требуется несколько повторений алгоритма для определения наилучшего значения ширины [1, 4].

Алгоритм кластерного ансамбля основан на множественных прогонах k-средних, чтобы собрать доказательства и избежать ложной классификации аномальных данных. В нем использована двухуровневая архитектура, основанная на алгоритмах обучения без контроля, первый из которых представляет собой алгоритм кластеризации без контроля, который уменьшает полезную нагрузку сетевого пакета до приемлемого размера. Вторым уровнем в их архитектуре является традиционный алгоритм обнаружения аномалий.

Методы интеллектуального анализа данных используются как в конструкции объекта, так и в классификации. Эти методы основаны на немаркированных данных. Для выявления важных входных признаков была разработана схема построения статистических признаков, в которой факторный анализ сочетается с оптимизированной техникой кластеризации k-средних. В качестве основного компонента для обнаружения неконтролируемых аномалий предложенная схема построения статистических признаков исключает оптимальное избыточное дублирование элементов путем рассмотрения сходства откликов элементов с помощью кластерного анализа, основанного на пространстве признаков, уменьшенном с помощью факторного анализа, который организовывает хорошее подмножество признаков, имеющих решающее значение для улучшения производительности классификаторов. Эффективность предложенного метода оценивается с использованием различных наборов данных, уменьшенных за счет ранжирования важности входных функций. Классификация вторжений по сокращенному пространству признаков основана на самоорганизующейся карте – методе для обучения без учета, который базируется на сетке искусственных нейронов, веса которых адаптированы для соответствия входным векторам в обучающем наборе.

Построение функции включает в себя процессы определения доказательств, которые можно извлечь из необработанных данных, наиболее полезных для анализа. Таким образом, создание объектов является критически важным шагом в построении системы обнаружения вторжений. Чтобы исключить избыточность признаков и улучшить классификацию путем поиска подмножества признаков, которые наилучшим образом классифицируют данные обучения, используются статистические методы, включая факторный анализ, который является одним из наиболее широко используемых методов уменьшения размерности, и k-средних кластеризация, которая имеет преимущество низкой временной сложности.

Факторный анализ – это статистический метод, используемый для выявления относительно небольшого числа факторов, которые могут представлять отношения между наборами многих взаимосвязанных переменных. Это уменьшает пространство атрибутов от большего числа переменных до меньшего числа факторов [3]. Факторный анализ создает таблицу, в которой строки представляют собой необработанные переменные индикатора, а столбцы – факторы, объясняющие, как можно большую разницу в этих переменных. Ячейки в этой таблице представляют собой факторные нагрузки, и значение факторов должно быть обусловлено наблюдением того, какие переменные наиболее сильно нагружены определенными факторами. Факторные нагрузки являются корреляцией между переменными и факторами.

В факторной аналитической модели p-мерный набор наблюдаемых переменных $x = (x_1, x_2,..., x_p)^T$ со значениями $\mu = (\mu_1, \mu_2,..., \mu_p)^T$ и ковариационной матрицей Σ представлен как линейные комбинации m ($m<<p$) скрытых переменных, называемые общими множителями $f = (f_1, f_2,..., f_m)^T$ вместе с p

дополнительными источниками вариации $\varepsilon = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p)^T$:

$$\begin{aligned} x_1 - \mu_1 &= \lambda_{11}f_1 + \lambda_{12}f_2 + \ldots + \lambda_{1m}f_m + \varepsilon_1 \\ x_2 - \mu_2 &= \lambda_{21}f_1 + \lambda_{22}f_2 + \ldots + \lambda_{2m}f_m + \varepsilon_2 \\ &\ldots \\ x_p - \mu_p &= \lambda_{p1}f_1 + \lambda_{p2}f_2 + \ldots + \lambda_{pm}f_m + \varepsilon_p. \end{aligned} \quad (1)$$

При записи в матричном виде:

$$x - \mu = \Delta f + \varepsilon, \quad (2)$$

где матрица загрузки:

$$\Delta = \begin{bmatrix} \lambda_{11} & \lambda_{12} & \ldots & \lambda_{1m} \\ \lambda_{21} & \lambda_{22} & \ldots & \lambda_{2m} \\ \vdots & \vdots & & \vdots \\ \lambda_{p1} & \lambda_{p2} & \ldots & \lambda_{pm} \end{bmatrix}.$$

Коэффициенты λ_{ij}, называемые загрузкой i-й переменной по j-му коэффициенту, выражают ковариацию между переменной x_i и фактором f_j. I-й удельный коэффициент ε связан только с i-й переменной xi. Предполагается, что значения f и ε удовлетворяют следующим условиям:

$E(f) = 0$, $Cov(f) = E(ff^T) = I$,
$E(\varepsilon) = 0$, $Cov(\varepsilon) = E(\varepsilon\varepsilon^T) = \Psi = diag(\psi_1, \psi_2, \ldots, \psi_p)$,
$Cov(\varepsilon, f) = E(\varepsilon f^T) = 0$.

Подходы, основанные на кластеризации, направлены на разделение данных на несколько кластеров, в которых каждой точке данных может быть назначена степень принадлежности к каждому из кластеров. Процесс формирования кластеров включает в себя объединение нескольких переменных в меру неоднородности или расстояния, значения которых затем используются для формирования групп. Напомним, кластеризация k-средних – это хорошо известный алгоритм кластеризации, который группирует n точек данных в k непересекающихся подмножеств Sj, чтобы минимизировать следующую целевую функцию суммы квадратов:

$$E = \sum_{j=1}^{k} \sum_{n \in S_j} |x_n - \mu_j|^2, \quad (3)$$

где x_n – вектор, представляющий n-ю точку данных;
μ – центр тяжести точек данных в Sj.

Популярность алгоритма k-средних обусловлена его простотой, малой временной сложностью и быстрой сходимостью. Алгоритм k-средних показан ниже:

- инициализировать $\mu_1, \ldots, \mu_K$ путем случайного выбора, пока в кластерах Sj не происходит никаких изменений для i = 1, … , n;
- рассчитать $|x_i - \mu_i|^2$ для всех центров;
- назначить точку данных i ближайшему центру;
- конец.

При применении факторного анализа, если построение элемента основано только на степени вклада, вызванного наблюдением того, какие переменные наиболее сильно загружены определенными факторами, выбранные элементы могут быть избыточными, поскольку информация, которую они включают в себя, содержится в других преимуществах. Эту избыточность можно уменьшить, если учесть сходство переменных ответов с набором обучающих данных с помощью кластерного анализа.

Поэтому предлагается схема построения статистического признака, в которой факторный анализ и кластеризация k-средних объединены в качестве основного компонента для обнаружения неконтролируемых аномалий. Этот метод направлен на оптимальное исключение избыточности в конструкции объекта и тем самым способствует обнаружению в реальном времени. Данная схема построения статистического признака выполняется в семь этапов.

В предложенной схеме первоначально используется факторный анализ, а затем алгоритм кластеризации k-средних применяется к каждому набору обучающих данных. На основе k кластеров (подмножество CA_1) признаков посредством кластеризации k-средних извлекаются признаки (подмножество CSjl), в которых нагрузки факторов выше определенного порога. Избыточность функций с высоким значением факторных нагрузок затем уменьшается, если они находятся в одном кластере, что обеспечивает правильную выборку (подмножество $FA_j(M)$) функций, критически важных для производительности классификаторов. Главным плюсом предлагаемой схемы построения объектов является то, что этот метод может иерархически уменьшать характеристики, что помогает ранжировать важность входных объектов с низкой сложностью по времени.

Алгоритм и процедура предложенной схемы построения признаков приведены ниже. Метод обнаружения неконтролируемых аномалий использует самоорганизующуюся карту для построения профилей нормального поведения и атак. Для обработки данных в режиме реального времени для классификации считается, что самоорганизующаяся карта наиболее выполнима благодаря следующим характеристикам:

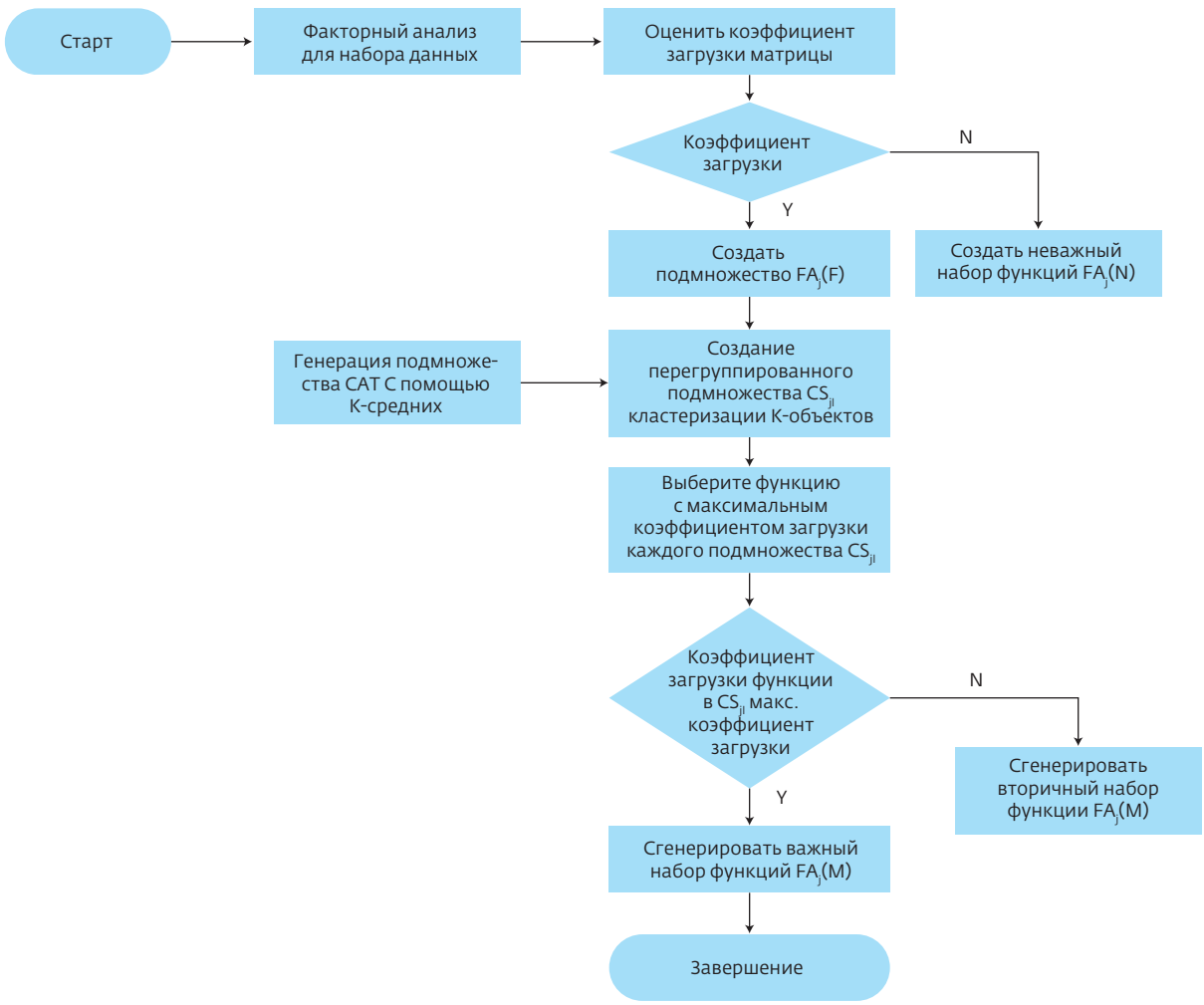


Рис.1. Функция построения процедуры

- высокая скорость конвертации по сравнению с другими методами обучения;
- алгоритм, основанный на обучении без учителя;
- обучение полностью ориентировано на данные.

Алгоритм построения схемы статистического признака показан на рис.1.

Ввод: набор данных x, $x = (x_1, x_2, \ldots x_p)^T$.

Вывод: подмножество CS_{jl}, $FA_j(S)$, $FA_j(N)$.

Шаг 1: Вычислить матрицу загрузки коэффициентов набора данных x.

Шаг 2: Для множителя $f_j(j = 1, 2,\ldots, m)$ сгенерировать подмножество $FA_j(F) = \{x_i|, x_i$ имеет коэффициент нагрузки $l_{ij} \geq \theta, i = 1, 2,\ldots, p\}$.

Шаг 3: Для фактора f_j $(j = 1, 2,\ldots, m)$ создается подмножество, представляющее незначительный набор функций $FA_j(M) = \{x_i|, x_i$ имеет коэффициент нагрузки $l_{ij}<\theta\}$.

Шаг 4: Генерация k-кластеров p-объектов, CA_l с помощью k-средних кластеров.

Шаг 5: Переставить матрицу факторной загрузки и сгенерировать подмножество CS_{jl} функций для коэффициента fj $(j = 1, 2,\ldots, m)$ и $l = 1, 2,\ldots, k$.

Шаг 6: Выбрать максимальное значение l_{jl} для каждого подмножества CS_{jl}и сгенерировать подмножество $FA_j(M) = \{x_i|, x_i$ имеет максимальный коэффициент загрузки $l_{jl}, l = 1, 2,\ldots, k\}$.

Шаг 7: Сгенерировать подмножество $FA_j(S) = \{x_i|, x_i$ не имеет максимального коэффициента загрузки l_{jl}, $l = 1, 2,\ldots, k\}$.

Сегодня самоорганизующаяся карта – это одна из самых популярных моделей нейронных сетей. В отличие от сетей, основанных на контролируемом обучении, которые требуют, чтобы целевые значения, соответствующие входным векторам, были известны, карту мы можем использовать для кластеризации данных, не зная членов класса входных данных. Следовательно, ее можно применять, чтобы обнаружить особенности, присущие проблеме. Кроме того, возможно реализовать упорядоченное отображение размерности, уменьшающее отображение обучающих данных. При этом карта следует функциям плотности вероятности данных.

Карта состоит из нейронов, расположенных на регулярной низкоразмерной сетке. Каждому нейрону в ней назначен связанный вектор веса. Любой заданный входной вектор сравнивается с вектором веса каждого нейрона, и ближайший нейрон объявляется победителем.

На каждом этапе обучения выборочный вектор выбирается случайным образом из набора входных данных. Наилучшая единица соответствия для входного вектора определяется на основе евклидова расстояния. Затем наилучшая единица соответствия и его топологические соседи перемещаются ближе к входному вектору во входном пространстве. Степень движения вектора веса определяется скоростью обучения α. Количество единиц, затронутых адаптацией, определяется функцией соседства h_{ci}. В связанном эксперименте используется функция окрестности Гаусса. Функция соседства определяется по формуле:

$$h_{ci}(t) = \exp\left(-\frac{||r_c - r_i||}{2\sigma^2(t)}\right), \quad (4)$$

где: rc и ri – положения нейронов на сетке карты;

σ – размер окрестности.

Скорость обучения и радиус окрестности являются убывающими функциями времени t.

Рассмотрим процедуру классификации. В качестве основы для классификатора используются U-матрица и гистограмма попадания. U-матрица показывает расстояния между соседними единицами и, таким образом, визуализирует кластерные структуры карты. Высокие значения в U-матрице обозначают большое расстояние между соседними единицами карты, а также указывают границы кластера. Можно проанализировать отношения между входными шаблонами в соответствии с расположением их изображений на карте и узнать, какие шаблоны намного ближе или похожи друг на друга в своем исходном пространстве.

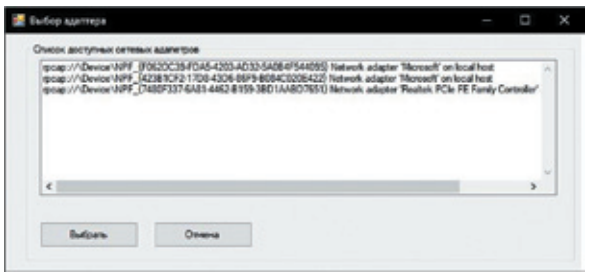


Рис.2. Окно выбора сетевого адаптера

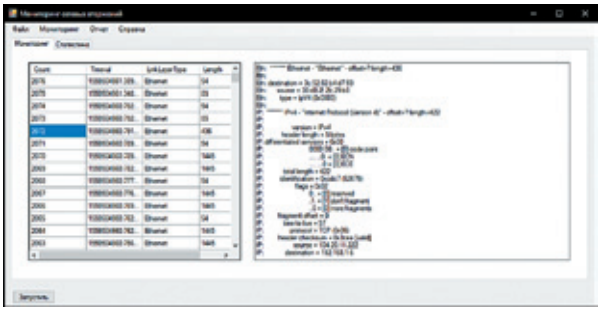


Рис.3. Программа в режиме мониторинга

Гистограмма попадания – важный инструмент для анализа данных с использованием карты. Она формируется путем нахождения наилучшей единицы соответствия каждой выборки данных на карте и увеличения счетчика в единице карты каждый раз, когда это подтверждается.

Чтобы определить, является ли сетевое соединение нормальным, для классификации в качестве параметра используется значение высоты U-матрицы. Сначала для классификации применяется порог. Если значение высоты превышает пороговое значение, оно классифицируется как аномальное. После того, как структура карты и матрица значений высоты получены, классификация проходит в четыре основных этапа.

Процесс обучения самоорганизующейся карты представлен пошагово ниже.

Шаг 1: Построить матрицу весов.

Шаг 2: Инициализировать матрицу весов с произвольно выбранными входными векторами.

Шаг 3: Для каждого входного вектора x:

- вычислить dist (x, i) = || x (t) – mi(t) ||;
- выбрать победителя в качестве нейрона c, $m_c(t) = min_i$|| x(t) – mi(t) ||, где каждый нейрон является вектором-прототипом, а n-мерный вектор mi = [m_{i1},..., m_{in}].

Шаг 4: Отрегулировать веса для победителя и всех его соседей:

$$m_c(t+1) = m_i(t) + \alpha(t) \cdot h_{ci}(t)|x(t) - m_i(t), \quad (5)$$

где: α (t) – скорость обучения;

$h_{ci}(t)$ – функция ядра окрестности с центром в блоке победителя.

Шаг 5: Уменьшить скорость обучения и размер соседства.

Шаг 6: Повтор шагов (2) – (5) до тех пор, пока критерий сходимости не будет удовлетворен.

Алгоритм классификации карты таков:

Шаг 1: Для каждого вектора характеристик сетевого трафика рассчитать значение веса для каждого нейрона, используя U-матрицу.

Шаг 2: Рассматривая компромисс между частотой обнаружения и частотой ложных тревог, рассчитать порог σ.

Шаг 3: Классифицировать вектор характеристик сетевого трафика как:

- ненормальный, если вес нейрона > σ;
- нормальный, если вес нейрона < σ.

Шаг 4: Генерация выходных данных классификатора самоорганизующейся карты.

Программное средство "Мониторинг сетевых вторжений" предназначено для мониторинга трафика в компьютерной сети организации или предприятия и обнаружения вторжений.

Для работы с программой пользователь должен обладать минимальными навыками работы с операционной системой семейства Windows, а также для понимания выполняемых действий иметь представление о возможных действиях, которые необходимо предпринять для изоляции вторжения.

Программа не нуждается в установке на компьютер и запускается сразу путем двойного нажатия на исполняемый файл.

Функциональные возможности программы "Мониторинг сетевых вторжений" состоят в мониторинге трафика, проходящего через компьютер, с которого происходит съем сетевых пакетов, а также (при наличии исходного кода) в возможности задания специальных значений для выполнения исследования криптостойкости протокола.

Алгоритм работы с программой:

22-25 июня

I международная выставка индустрии безопасности

НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ БЕЛАРУСЬ★2022

ОРГАНИЗАТОРЫ ВЫСТАВКИ:

Государственный секретариат Совета Безопасности Республики Беларусь

Управление делами Президента Республики Беларусь

Национальный выставочный центр «БелЭкспо»

- ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА
- СИСТЕМЫ И КОМПЛЕКСЫ МОНИТОРИНГА ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ, ОБЕСПЕЧЕНИЯ ПРОФИЛАКТИКИ ПРАВОНАРУШЕНИЙ И ЗАЩИТЫ ГРАЖДАН
- СИСТЕМЫ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ, УЯЗВИМЫХ В ТЕРРОРИСТИЧЕСКОМ ОТНОШЕНИИ
- ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ ГРАНИЦЫ
- СПЕЦИАЛЬНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ И СПЕЦСЛУЖБ
- ТЕХНИЧЕСКИЕ СРЕДСТВА И СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ АВАРИЙ, КАТАСТРОФ И ЛИКВИДАЦИИ ИХ ПОСЛЕДСТВИЙ
- СПЕЦИАЛЬНЫЕ СРЕДСТВА ПОЖАРНОЙ БЕЗОПАСНОСТИ
- ОБОРУДОВАНИЕ И КОМПЛЕКТУЮЩИЕ, ИСПОЛЬЗУЕМЫЕ В МЕДИЦИНЕ КАТАСТРОФ
- СРЕДСТВА ОБЕСПЕЧЕНИЯ ПРОМЫШЛЕННОЙ, ЭКОЛОГИЧЕСКОЙ И ЭПИДЕМИОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

МИНСК-АРЕНА
пр-т Победителей,111

nbbexpo.by

```
Eth:  ******* Ethernet - "Ethernet" - offset=? length=436
Eth:
Eth: destination = 3c:52:82:b4:d7:69
Eth:     source = 38:d8:2f:2b:29:b8
Eth:       type = IpV4 (0x0800)
Eth:
IP:  ******* IPv4 - "Internet Protocol (Version 4)" - offset=? length=422
IP:
IP:             version = IPv4
IP:         header length = 5 bytes
IP: differentiated services = 0x00
IP:                   0000 00.. = [0] code point
IP:                   .... ..0. = [0] ECN
IP:                   .... ...0 = [0] ECE
IP:          total length = 422
IP:        identification = 0xcdc7 (52679)
IP:                 flags = 0x02
IP:                   0.. = [0] reserved
IP:                   .1. = [1] don't fragment
IP:                   ..0 = [0] more fragments
IP:       fragment offset = 0
IP:          time to live = 57
IP:              protocol = TCP (0x06)
IP:       header checksum = 0x3cea [valid]
IP:                source = 104.20.11.222
IP:           destination = 192.168.1.6
```

Рис.4. Информация по перехваченному сетевому пакету

- выбрать один из сетевых адаптеров (рис.2);
- установить необходимые значения для пороговых значений, если есть такая необходимость;
- в режиме аудита, при необходимости, просмотреть содержимое пакета.

Интерфейс программы разделен на две основные формы. На первой происходит отображение перехватываемого потока сетевых пакетов. На вспомогательной осуществляется выбор доступного сетевого адаптера.

Каждый сетевой пакет можно изучить, выбрав его в окне, и получить всю доступную информацию о нем, что иллюстрируется на рис.3 и 4.

В случае превышения одного из установленных пороговых значений рассматриваемая программа выдаст соответствующее предупреждение.

Заключение

Из-за растущего числа потенциальных уязвимостей в системах безопасности организаций специалистам в области информационной защиты необходимо постоянно снижать риски, связанные с быстро меняющейся информационной средой. Рассмотренные в статье методы являются незаменимыми инструментами, но необходимо понимать, что они не способны самостоятельно заменить весь спектр методов и средств информационной безопасности.

Выбор одной технологии для комплексной защиты приводит к неоправданно высокому риску. Объединив несколько мер защиты, организации могут обеспечить надежный уровень безопасности от различных типов атак и вредоносных воздействий, тем самым снизив потенциальный риск до приемлемого уровня.

ЛИТЕРАТУРА

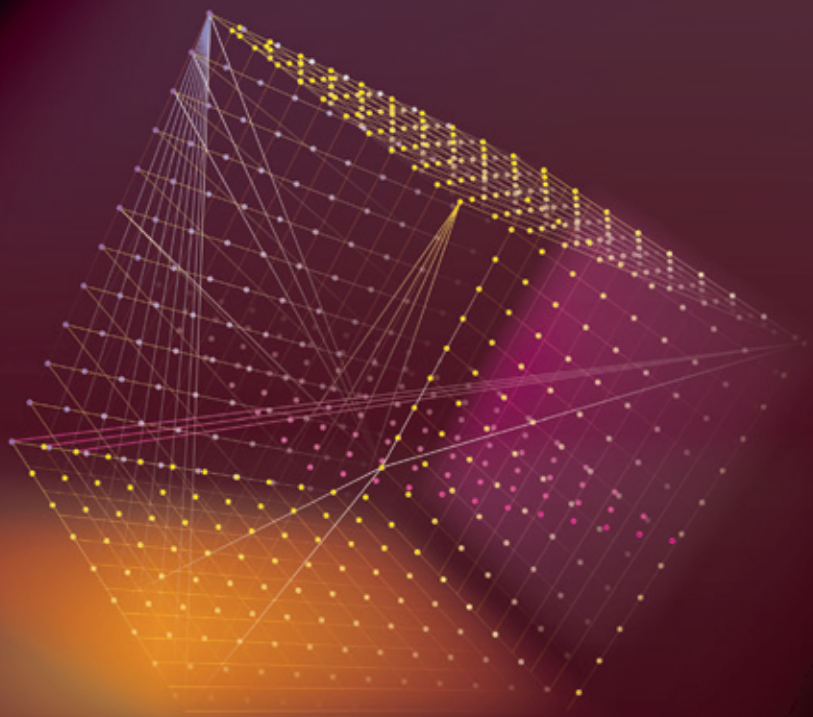
1. Автоматизированный способ обнаружения компьютерных атак на сетевую компьютерную систему [Электронный ресурс]. URL: http://www.findpatent.ru/patent/253/2538292.html (дата обращения: 25.11.2021).
2. **Фаткиева Р.Р., Атисков А.Ю., Левоневский Д.К.** Автоматизированное рабочее место для мониторинга и прогнозирования вторжений // Патент РФ № 139517U1. 2014. Бюл. № 11.
3. **Бельков Д.В., Едемская Е.Н., Незамова Л.В.** Статистический анализ сетевого трафика // Информатика, кибернетика и вычислительная техника. 2011. № 13. С. 66–75.
4. **Гребенников А.В., Крюков Ю.А., Чернягин Д.В.** Моделирование сетевого трафика и прогнозирование с помощью модели ARIMA // Электронный журнал "Системный анализ в науке и образовании". 2011. № 1. С. 1–11.
5. **Корниенко А.А., Слюсаренко И.М.** Системы и методы обнаружения вторжений: современное состояние и направления совершенствования [Электронный ресурс]. URL: http://citforum.ru/security/internet/ids_overview (дата обращения: 25.11.2021).
6. Система обнаружения и предотвращения вторжений на основе контроля доступа к ресурсам [Электронный ресурс]. URL: http://www.findpatent.ru/patent/254/2543564.html (дата обращения: 25.11.2021).
7. Современное состояние проблемы обнаружения сетевых вторжений [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-problemy-obnaruzheniya-setevyh-vtorzheniy (дата обращения 25.11.2021).
8. **Bennett S.P., Kailay M.P.** An application of qualitative risk analysis to computer security for the commercial sector // Eighth Annual IEEE Computer Security Applications Conference. 2018. No. 4. PP. 64–73.
9. **Mayer N., Matulevicius R., Heymans P.** Alignment of Misuse Cases with Security Risk Management // Proceedings of the 2018 International Conference on Availability, Reliability and Security. 2018. PP. 1397–1404. Транспорт Урала

interlight
RUSSIA
intelligent building
RUSSIA

19 – 22.09.2022
ЦВК «ЭКСПОЦЕНТР», МОСКВА

Умная. Светлая. Стильная.

Международная выставка освещения, автоматизации зданий, электротехники и систем безопасности



ТЕХНОСФЕРА
РЕКЛАМНО-ИЗДАТЕЛЬСКИЙ ЦЕНТР

100% ГАРАНТИЯ
ПОЛУЧЕНИЯ ВСЕХ НОМЕРОВ

Стоимость 2200 р. за номер
Периодичность: 10 номеров в год
www.electronics.ru

Стоимость 1450 р. за номер
Периодичность: 8 номеров в год
www.photonics.su

Стоимость 1450 р. за номер
Периодичность: 6 номеров в год
www.j-analytics.ru

ПОДПИСКА НА ЖУРНАЛЫ

www.technosphera.ru

Стоимость 1300 р. за номер
Периодичность: 8 номеров в год
www.lastmile.su

Стоимость 1300 р. за номер
Периодичность: 8 номеров в год
www.nanoindustry.su

Стоимость 1800 р. за номер
Периодичность: 4 номера в год
www.stankoinstrument.su