Инженерный вестник Дона, №2 (2026)
ivdon.ru/ru/magazine/archive/n2y2026/10745

Методы защиты от атаки Сибиллы на основе анализа коррелограммы карты мощности электромагнитного поля сетевого трафика

В.В. Ерохин[1,2], *А.В. Аксенов*[1]

[1]*МИРЭА – Российский технологический университет*
[2]*Московский государственный институт (университет) международных отношений Министерства иностранных дел Российской Федерации*

Аннотация: Рассматривается метод противодействия атаке Сибиллы в распределённых системах, основанный на анализе карты мощности электромагнитного излучения временны́х характеристик сетевого трафика. Ключевая гипотеза заключается в том, что множество сибел-идентификаторов, управляемых одним узлом-злоумышленником, демонстрирует статистически значимую корреляцию в паттернах своей сетевой активности, которая может быть выявлена с помощью коррелограммы. Предложен метод обнаружения атаки Сибиллы в беспроводных сетях на основе анализа коррелограмм карт мощности электромагнитного сигнала. Метод использует статистические свойства профилей мощности, возникающие из-за коррелированности сетевой активности сибел-узлов, управляемых одним злоумышленником. Разработана архитектура системы защиты, включающая модули мониторинга сетевой активности, вычисления коррелограмм, кластеризации и детектирования аномалий. Введен комплекс из 10 параметров коррелограмм для идентификации атак, включая дисперсию профиля, коэффициенты случайности и периодичности, спектральную плотность и корреляционные характеристики. Экспериментальная проверка на радиолокационной станции миллиметрового диапазона показала точность обнаружения от 83,2% до 97,4%. Для повышения эффективности метода предложено использование глубоких нейронных сетей после накопления достаточного объема данных. Предлагаемый метод позволяет идентифицировать и отсекать скомпрометированные идентификаторы, повышая устойчивость P2P-сетей, блокчейн-систем и распределённых реестров.
Ключевые слова: атака Сибиллы, безопасность распределённых систем, коррелограмма, анализ сетевого трафика, временны́е ряды, автокорреляция, обнаружение аномалий.

Введение

Атака Сибиллы – это разновидность угроз кибербезопасности, при которой злоумышленник создаёт и применяет большое число псевдонимных идентификаторов (сибел-узлов) с целью получить непропорциональное влияние в сети. Такой подход ставит под угрозу основы децентрализованных систем, и приводит к следующим эффектам:

- манипуляциям с консенсусом (например, в блокчейне);
- искажению результатов голосований;
- снижению эффективности механизмов оценки репутации;

- ухудшению маршрутизации в P2P-сетях.

Типичные методы защиты, такие как механизмы консенсуса на основе доказательства выполненной вычислительной работы (Proof-of-Work), доказательства доли участия в системе (Proof-of-Stake) либо методы криптографической сертификации, нередко сопровождаются значительными вычислительными или организационными расходами. В предлагаемой работе рассматривается пассивный метод обнаружения на основе наблюдения за атакой, основанный на естественных свойствах самой атаки. Гипотеза состоит в существовании корреляции между трафиком: физический узел злоумышленника ограничен по ресурсам (процессорное время, пропускная способность канала). Управляя множеством сибел-идентификаторов, его сеточная активность (отправка сообщений, пинги, транзакции) с высокой долей вероятности инициируется из одного источника. Это вызывает корреляцию во временных рядах активности этих идентификаторов.

Принцип обнаружения атаки. При активности незаависимых узлов их временные ряды (например, число пакетов за единицу времени) карты мощности электромагнитного излучения сетевого трафика, излучаемых передатчиками, будут обладать различными, несвязанными коррелограммами. В то же время сибел-идентификаторы, контролируемые одним узлом, демонстрируют сходные паттерны автокорреляции. Это объясняется следующими факторами:

1. Общий источник генерации событий: запросы разных сибел-идентификаторов могут поступать почти одновременно.
2. Общий сетевой интерфейс: все пакеты проходят через один канал, что вызывает общие задержки и характерные паттерны потерь.
3. Периодичность активности: управляющая программа или скрипт для сибел-узлов может использовать внутренние таймеры, вызывая синхронизированные всплески активности.

Для комплексного описания профиля карты мощности принимаемого сигнала предлагается использовать корреляционную функцию. Данная функция представляет собой наиболее полную и эффективную интегральную характеристику, превосходящую по информативности такие параметры, как максимальная, минимальная и средняя мощность, а также угловые характеристики пиков и впадин.

Вычисление корреляционных функций применяется для обработки экспериментальных данных и позволяет решать задачу идентификации карт мощности. Это особенно актуально для сигналов от различных источников, имеющих схожие значения базовых параметров. Для случайной стационарной функции корреляционная функция определяется следующим выражением:

$$R_y(\tau) = \lim_{1-\tau\to 0}\left(\frac{l}{l-\tau}\right)\int_0^{l-\tau}(y(x)-M)(y(x+\tau)-M)dx, \quad (1)$$

где τ – переменная разность между абсциссами двух сечений профилограммы карты мощности; l – длина профилограммы карты мощности; $y(x)$, $y(x+\tau)$ – ординаты профилограммы карты мощности в выбранной системе координат; M – математическое ожидание профилограммы карты мощности в выбранной системе координат.

Метод обнаружения атаки Сибиллы на основе анализа кореллограммы карты мощности электромагнитного сигнала сетевого трафика

Архитектура системы защиты состоит из следующих модулей:

1. Модуль "Монитор сетевой активности". Этот модуль собирает временны́е ряды для каждого идентификатора в сети. Параметры ряда: количество

исходящих пакетов, размер отправленных данных, количество установленных соединений за заданный временной интервал (например, 1 секунда).

2. Модуль "Вычислитель коррелограмм". Здесь для каждого нового идентификатора или при подозрении строится временной ряд достаточной длины (например, 1000 наблюдений) и вычисляется его коррелограмма до заданного лага, например, лага K=20.

3. Модуль "Кластеризация и сравнение". В этом модуле рассчитанные коррелограммы для всех активных идентификаторов сравниваются между собой. Используются метрики расстояния между функциями, такие как евклидово расстояние или динамическое искривление времени (Dynamic Time Warping - DTW), для учета возможных незначительных временны́х сдвигов.

4. Модуль "Детектор аномалий". Идентификаторы, чьи коррелограммы образуют плотные кластеры с высокой степенью схожести, классифицируются как сибел-узлы, принадлежащие одному злоумышленнику. Для принятия решения применяются пороговые значения либо алгоритмы машинного обучения без учителя (например, алгоритм пространственной кластеризации на основе плотности с учётом шума (Density-Based Spatial Clustering of Applications with Noise — DBSCAN)).

В данном исследовании интеграл (1) заменяет конечной суммой:

$$R_y(\tau) = \frac{l}{l-\tau}\sum_{0}^{l-\tau}(y(x)-\bar{y})(y(x+\tau)-\bar{y})\Delta x, \qquad (2)$$

где $\bar{y}$ – среднее значение ординаты профилограммы карты мощности в выбранной системе координат; Δx – интервал (все интервалы имеют одинаковую длину), на которые разбивается профилограмма карты

мощности для расчета корреляционной функции. Причем l и τ выражают в интервалах Δx. акже вместо корреляционной функции $R_y(\tau)$ часто пользуются ее нормированной величиной:

$$r_y(\tau) = \frac{R_y(\tau)}{D(y)}, \quad (3)$$

где $D(y)$ – дисперсия случайной величины $y(x)$.

Далее рассмотрим выбор минимальной длины профилограммы и ограничение длины коррелограммы.

Уравнение расчета минимальной длины профилограммы l_{min} при ее корреляционном преобразовании определяется по формуле:

$$l_{min} = 2\Delta x \frac{(\lambda - \delta)(4 - 3\delta)}{(1 - \delta)^2}, \quad (4)$$

где λ – коэффициент снижения случайности при корреляционном преобразовании профиля карты мощности (принимается в пределах от 5 до 10) [1-3]; δ – коэффициент случайности профиля профилограммы карты мощности, представляющий отношение дисперсий случайной составляющей к дисперсии реального профиля карты мощности.

$$\delta = \frac{D_\delta}{D}, \quad (5)$$

где D_δ – случайная составляющая дисперсии нормированного профиля профилограммы карты мощности; D – дисперсия нормированного профиля профилограммы карты мощности.

При очень большом τ коррелограмма дает ненадежную случайную информацию, т.к. снижается длина корреляционно преобразуемой профилограммы карты мощности. Поэтому длину τ следует ограничить:

$$\tau_{max} = \Delta x(\lambda_{max} - \lambda_{min})\frac{4-3\delta}{(1-\delta)^2}, \quad (6)$$

где λ_{max} и λ_{min} – соответственно максимальный и минимальный коэффициенты снижения случайности при корреляционном преобразовании. В зависимости от рельефа местности, типа передатчика электромагнитного сигнала, мощности передаваемого электромагнитного сигнала и погодных условий, при которых эта профилограмма карты мощности была получена, коэффициент δ находится в пределах от 0 до 1. Коэффициент δ определяет степень приближения закона распределения реального профиля к нормальному, чем ближе коэффициент δ к 1, тем ближе закон распределения к нормальному. Условно можно разделить профили карты мощности в зависимости от вида закона распределения и значения коэффициента δ на систематические ($\delta < 0{,}4$), гибридные ($0{,}4 < \delta < 0{,}65$) и случайные ($\delta > 0.7$). Поскольку расположение, высотные и шаговые параметры пиков и впадин профилограммы карты мощности носит случайный характер, то для изучения свойств профилограмм и для интегрированной оценки идентификации карты мощности могут быть использованы методы теории случайных функций. С точки зрения этой теории, профиль карты мощности может быть рассмотрен как совокупность систематической и случайной вставляющих, причем последняя является реализацией случайной стационарной функцией, определяющей распределения пиков и впадин карты мощности. Стационарность профиля карты мощности характеризуется тем, что при стабильных условиях передачи электромагнитного сигнала источником

коррелограммы карты мощности имеют вид непрерывных колебаний относительно некоторого среднего значения. Причем ни средняя амплитуда электромагнитных колебаний, ни характер колебаний не позволяют обнаружить существенных изменений профиля карты мощности.

Целесообразно для дальнейших вычислений использовать нормированную корреляционную функцию, где дисперсия D при значении аргумента корреляционной функции τ =0 вычисляется по формуле:

$$D = \frac{l}{l-\tau}\sum_{x=l}^{l-\tau}(y(x)-\bar{y})(y(x+\tau)-\bar{y})\Delta x, \qquad (7)$$

Для снижения дисперсии оценка корреляционной функции подвергается взвешенному сглаживанию во временной области с применением корреляционного окна (lag window), методология которого была систематизирована по методу Блэкмана-Тьюки [4-5]. Данная процедура осуществляет усреднение функции в окрестности каждого временного лага, назначая большие веса ближайшим значениям и подавляя вклад удалённых лагов, что позволяет управлять компромиссом между разрешающей способностью и дисперсией оценки. Однако, следует отметить, что корреляционная функция, сама по себе, не обеспечивает полной идентификации карты мощности. Поэтому для решения данной задачи применяется комплексный подход, сочетающий количественный анализ корреляционных характеристик с визуализацией в виде коррелограмм (рис. 1 и рис. 2), что позволяет получить как интегральные метрики, так и наглядное представление о временной структуре сигнала, что будет рассмотрено далее. В соответствии с современными рекомендациями по спектральному анализу [4, 6, 7], в данной работе для сглаживания была выбрана весовая функция Тьюки. Её использование предпочтительно в связи с меньшим смещением

(bias) по сравнению с альтернативами, что обеспечивает более быструю стабилизацию выборочной спектральной плотности и сокращает требуемую длину реализации для достижения состоятельности оценки.

Далее излагается применение спектрального метода, основанного на описанной процедуре, для решения задачи идентификации профилей карт мощности. Для повышения удобства анализа и повышения точности (ограничение рассмотрено ниже) результата идентификации карты мощности дополним коррелограмму спектрограммой.

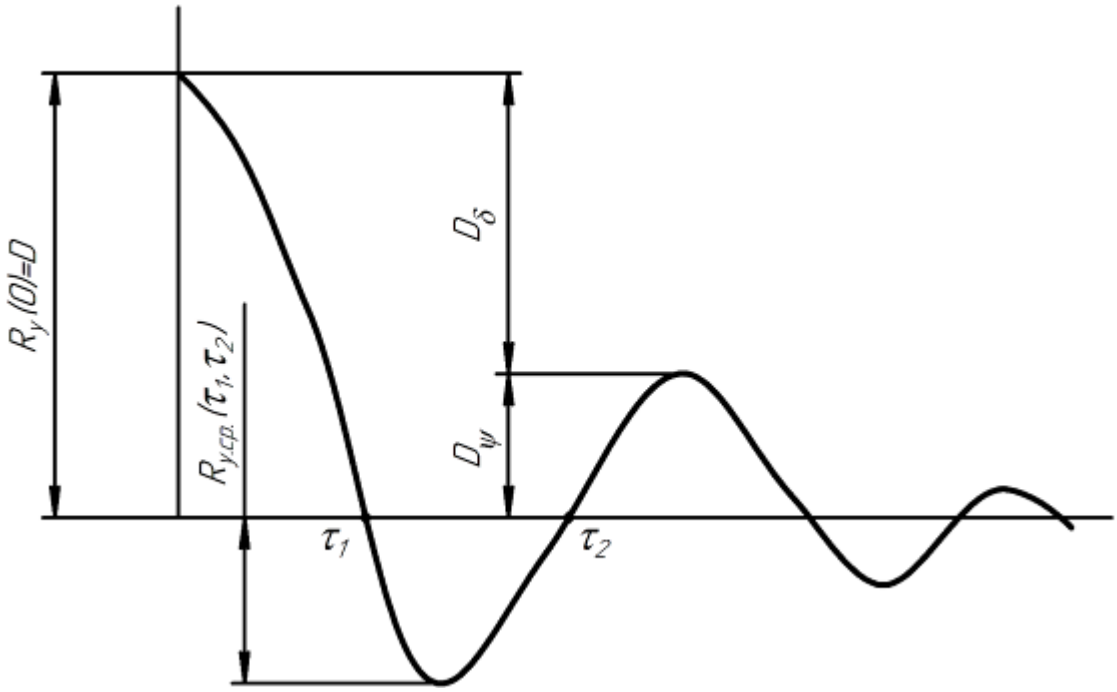

Рис. 1. Схема расчета коррелограммы карты мощности

Спектральная плотность $G(\omega)$ – это функция, описывающая распределение дисперсий пиков и впадин профилограммы карты мощности по частотам. Она показывает, какой конфигурации пики и впадины профилограммы карты мощности преобладают в данном профиле, какова её внутренняя структура. Представить новую информацию, отличной от информации, корреляционной функцией, спектрограмма не может, т.к. она является преобразованием корреляционной функции.

$$G(\omega) = \frac{0,5}{\pi} \int_{-\infty}^{+\infty} R_y(\tau) \cos(\omega\tau)\, dt, \qquad (8)$$

где ω – частота образования пиков и впадин на профилограмме карты мощности. Несмотря на преимущество спектрограммы в визуальной интерпретации данных по сравнению с коррелограммой, её ключевым недостатком является низкая точность аппроксимации аналитическими моделями. В связи с этим, в рамках данного исследования спектрограммы применяются в качестве вспомогательного инструмента.

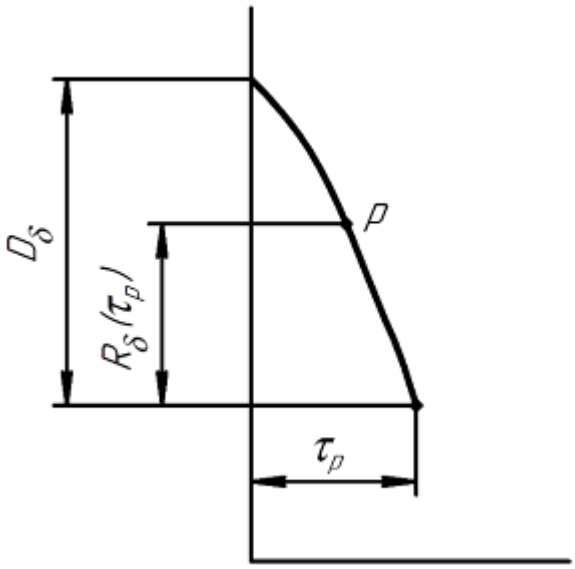

Рис. 2. Схема для расчета случайной составляющей коррелограммы профиля карты мощности

Их использование для идентификации коррелограмм целесообразно лишь в тех случаях, когда в профиле карты мощности на фоне стохастических колебаний наблюдается выраженная периодическая составляющая, проявляющаяся в виде дискретных гармоник.

И так для полной идентификации карты мощности используем следующие параметры:

1) *D* – дисперсия нормированного профиля карты мощности;

2) δ – коэффициент случайности профиля профилограммы карты мощности;

3) $\psi = (1 - \delta)$ – коэффициент периодичности профиля профилограммы карты мощности;

4) S_ψ – средний шаг периодической составляющей профиля коррелограммы карты мощности;

5) S_δ – средний шаг случайной составляющей профиля коррелограммы карты мощности;

6) S – средний шаг профиля профилограммы карты мощности;

7) $R_{y.cp.}(\tau_1, \tau_2)$ – среднее значение коррелограммы на начальном участке кривой коррелограммы при $R_y(\tau_1) = 0$ и $R_y(\tau_2) = 0$.

8) $G(\omega,n)$ – спектральная плотность с учетом окна Тьюки;

9) r_r – коэффициент корреляции коррелограмм.

10) σ_r – среднее квадратичное отклонение двух коррелограмм $R_{y1}(t)$ и $R_{y2}(t)$, где $R_{y1}(t)$ и $R_{y2}(t)$ –функции коррелограммы соответственно первой (эталонной или истинной) и второй (сравниваемой) карты мощности.

$$S_\psi = \frac{\sum_{i=1}^{m} S_{\psi i}}{m}, \tag{9}$$

где $S_{\psi i}$ – расстояние между точками пересечения коррелограммы с осью абсцисс; m – количество точек пересечения коррелограммы с осью абсцисс.

$$S_\delta = \frac{5\tau_p}{\sqrt{\left|\ln \frac{R_y(\tau_p)}{D_\delta}\right|}}, \tag{10}$$

где τ_p – абсцисса произвольной точки "p" на участке кривой коррелограммы, расположенной выше периодической части коррелограммы.

$$S = \frac{D}{\frac{D_\delta}{S_\delta} + \frac{D_\psi}{S_\psi}} \text{ или } S = \frac{S_\delta S_\psi}{S_\delta + S_\psi}. \quad (11)$$

$$R_{y.cp.} = R_y\left(\frac{\tau_1 + \tau_2}{2}\right). \quad (12)$$

$$G(\omega, n) = 2\Delta t\left(R_y(0) + 2\sum_{h=1}^{M_y-1} R_y(h\Delta t)\omega(h)\cos\left(\frac{2\pi hn}{N}\right)\right), \quad (13)$$

где n = 0, 1, 2, …, N/2; $\omega(h)$ – корреляционное окно Тьюки; $R_y(0)$ и $R_y(h\Delta t)$ – значение корреляционной функции при запаздываниях соответственно $\tau = 0$ и $\tau = h\Delta t$; N – общее количество значений в наборе данных профиля карты мощности.

$$\omega(h) = \begin{cases} 1 + \frac{\pi h}{N}, & \text{при } |h| \le N; \\ 0, & \text{при } |h| > N. \end{cases} \quad (14)$$

$$r_r = \frac{\overline{R_{y1}(t) \cdot R_{y2}(t)}}{\overline{R_{y1}(t)} \cdot \overline{R_{y2}(t)}}, \quad (15)$$

где $\overline{R_{y1}(t) \cdot R_{y2}(t)}$ – среднее значение произведения $R_{y1}(t) \cdot R_{y2}(t)$; $\overline{R_{y1}(t)}$ и $\overline{R_{y2}(t)}$ – среднее значение функций коррелограммы соответственно первой (эталонной или истинной) и второй (сравниваемой) карты мощности.

$$\sigma_r = \overline{R_{y1}(t)}\sqrt{1 - r_r^2}. \quad (16)$$

В таблице 1 представлены значения параметров коррелограмм для определения атаки Сибиллы.

В таблице параметр σ_r определяется следующим образом: σ_{r1} – среднее квадратичное отклонение двух коррелограмм $R_{y1}(t)$ и $R_{y1'}(t)$, либо среднее значение всех пар $R_{y1}(t)$ и $R_{y1'}(t)$, где $R_{y1}(t)$ – первая функция коррелограммы истинный карты мощности, $R_{y1'}(t)$ – другие измерения функции коррелограммы истинной карты мощности, например, при динамических преградах на пути сигнала от робота-клиента к роботу-серверу; σ_{r2} – среднее квадратичное отклонение двух коррелограмм $R_{y1}(t)$ и $R_{y2}(t)$, либо среднее значение всех пар $R_{y1}(t)$ и $R_{y2}(t)$, где $R_{y1}(t)$ – первая функция коррелограммы истинный карты мощности, $R_{y2}(t)$ – другие измерения функции коррелограммы анализируемой карты мощности. Таким образом, определяя и сравнивая параметры корреляционной функции, можно решить проблемы идентификации реальных карт мощностей. При этом используется база данных, в которую заносятся рассчитанные параметры корреляционных функции. Благодаря этому многопараметрическому методу идентификации, даже не зная при каких условиях был получен данный профиль карты мощности, можно его идентифицировать, т.е. либо он истинный, либо была атака Сибиллы.

Таблица 1. Значения параметров коррелограмм для определения атаки Сивиллы

Параметр коррелограммы	Наличие атаки Сибиллы	Истинный сигналы от роботов-клиентов
D	$\left\|\frac{D_1 - D_2}{D_1}\right\| \geq 0{,}05$	$\left\|\frac{D_1 - D_2}{D_1}\right\| < 0{,}05$
δ	$\left\|\frac{\delta_1 - \delta_2}{\delta_1}\right\| \geq 0{,}075$	$\left\|\frac{\delta_1 - \delta_2}{\delta_1}\right\| < 0{,}075$

ψ	$\left\|\frac{\psi_1-\psi_2}{\psi_1}\right\| \geq 0{,}075$	$\left\|\frac{\psi_1-\psi_2}{\psi_1}\right\| < 0{,}075$
S_ψ	$\left\|\frac{S_{\psi 1}-S_{\psi 2}}{S_{\psi 1}}\right\| \geq 0{,}10$	$\left\|\frac{S_{\psi 1}-S_{\psi 2}}{S_{\psi 1}}\right\| < 0{,}10$
S_δ	$\left\|\frac{S_{\delta 1}-S_{\delta 2}}{S_{\delta 1}}\right\| \geq 0{,}11$	$\left\|\frac{S_{\delta 1}-S_{\delta 2}}{S_{\delta 1}}\right\| < 0{,}11$
S	$\left\|\frac{S_1-S_2}{S_1}\right\| \geq 0{,}10$	$\left\|\frac{S_1-S_2}{S_1}\right\| < 0{,}10$
$R_{y.cp.}(\tau_1,\tau_2)$	$\left\|\frac{R_{y.cp.1}-R_{y.cp.2}}{R_{y.cp.1}}\right\| \geq 0{,}085$	$\left\|\frac{R_{y.cp.1}-R_{y.cp.2}}{R_{y.cp.1}}\right\| < 0{,}085$
$G(\omega,n)$	$\left\|\frac{G(\omega,n)_1-G(\omega,n)_2}{G(\omega,n)_1}\right\| \geq 0{,}15$	$\left\|\frac{G(\omega,n)_1-G(\omega,n)_2}{G(\omega,n)_1}\right\| < 0{,}15$
r_r	$r_r \leq 0{,}85$	$r_r > 0{,}85$
σ_r	$\left\|\frac{\sigma_{r1}-\sigma_{r2}}{\sigma_{r1}}\right\| \geq 0{,}75$	$\left\|\frac{\sigma_{r1}-\sigma_{r2}}{\sigma_{r1}}\right\| < 0{,}75$

Методика определения коррелограммы карты мощности состоит из шагов.

Исходные данные:

• набор профилей высот поверхности $h(x, y)$;

• в исследовании используется одномерная коррелограмма, для которой можно брать линейные профили по координате "y";

• единицы измерения высоты и расстояния между точками (шаг по координате "x").

Шаги расчёта:

1. Подготовка данных:

♦ если у вас двумерная карта высот $h(i)$, можно работать по двум направлениям, взяв одномерные профили;

♦ выбрать размер шага по пространству Δx;

♦ нормировка, здесь часто высоты центрируют в виде $h' = h - \text{mean}(h)$. Можно дополнительно нормировать по стандартному отклонению.

2. Расчет одномерной коррелограммы по профилю:

♦ возьмём одномерный профиль высот $h[k]$, $k = 0..N-1$;

♦ вычислим авто-корреляцию или корреляционную функцию по задержке τ: $R(\tau) = E[(h[k] - \mu)(h[k + \tau] - \mu)]$. При конечном наборе данных для нечётного τ (или по смещению) вычисляют эмпирическую корреляцию: $R(\tau) = (1/(N - \tau))$ $\sum\_\{k = 0\}^\{N - \tau - 1\}$ $(h[k] - \mu)(h[k + \tau] - \mu)$

♦ нормируем: $C(\tau) = R(\tau) / R(0)$, чтобы получить коэффициенты корреляции в диапазоне от −1 до 1.

♦ можно ограничиться τ от 0 до τ_{max}, где τ_{max} задаётся по физической размерности поверхности.

3. Дополнительно вычисляем спектр профиля через дискретное преобразование Фурье и оценивать среднюю пространственную частоту.

Ниже приведён пример расчёта и построения коррелограммы по одномерному профилю высот.

```
import numpy as np
import matplotlib.pyplot as plt

# Пример: синтетический профиль высот h
np.random.seed(0)
N = 1000
# создаём случайный профиль с заданной корреляцией
h = np.cumsum(np.random.randn(N))  # простой пример
h = h - h.mean()  # центровка

# параметры
mu = h.mean()
h_centered = h - mu

# авто корреляция по лагам τ = 0..N-1
lags = np.arange(0, N)
R = np.correlate(h_centered, h_centered, mode='full')
# корреляционная функция: взять правую половину и нормировать
R = R[N-1:]  # R[0]..R[N-1]
```

```
R_norm = R / R[0]

# график
plt.figure()
plt.plot(lags, R_norm, label='Авто корреляция')
plt.xlabel('Задержка τ')
plt.ylabel('C(τ) = R(τ)/R(0)')
plt.title('Коррелограмма одного профиля высот')
plt.grid(True)
plt.legend()
plt.show()
```

Общий алгоритм идентификации атаки Сибиллы:

1. Определяются на роботе-сервере эталонные или истинные параметры коррелограммы карты мощности робота-клиента [8].

2. В рабочем режиме роботом-сервером снимается параметры коррелограммы карты мощности робота-клиента, которые сравниваются со значениями в табл., определяющими атаку Сибиллы.

3. Создается дата-сет профилей истинных карт мощностей роботов-клиентов и профилей с атакой Сибиллы.

4. Когда дата-сет будет иметь более 1000 строк записей, тогда обучается искусственная глубокая нейронная сеть распознаванию атаки Сибиллы.

5. После обучения искусственной глубокой нейронной сети, эта сеть становиться также 11-м параметром идентификации атаки Сибиллы.

6. Если какой-либо из 11-и параметров идентифицирует атаку Сибиллы, тогда карта мощности робота-клиента считается скомпрометированной, т.е. она не является истинной.

7. Если время на распознавание атаки Сибиллы ограничено масштабом реального времени, тогда после обучения искусственной глубокой нейронной сети, она становиться единственным параметром, который будет идентифицировать атаку Сибиллы.

Экспериментальное подтверждение работоспособности метода обнаружения атаки Сибиллы на основе анализа кореллограммы карты мощности электромагнитного сигнала сетевого трафика

Экспериментальная установка состоит из робота-сервера "Радиолокационная станция обнаружения подвижных объектов на базе ФАР миллиметрового диапазона РЛС-01". Система из роботов-клиента аналогична из источника [8].

Был создан программный комплекс по мониторингу карты мощности электромагнитного сигнала сетевого трафика передатчиков роботов-клиентов (рис. 3, рис. 4, рис. 5). Были определены параметры кореллограммы согласно таблицы, которые показали точность метода от 83,2% до 97,4%. Наибольшая точность метода достигает, когда имеются статические препятствия в виде стен, преград и других физических объектов. В этом случае достаточно много отражающих сигналов приходит на робот-сервер, что позволяет иметь карту мощности с большим количеством пиков и впадин.

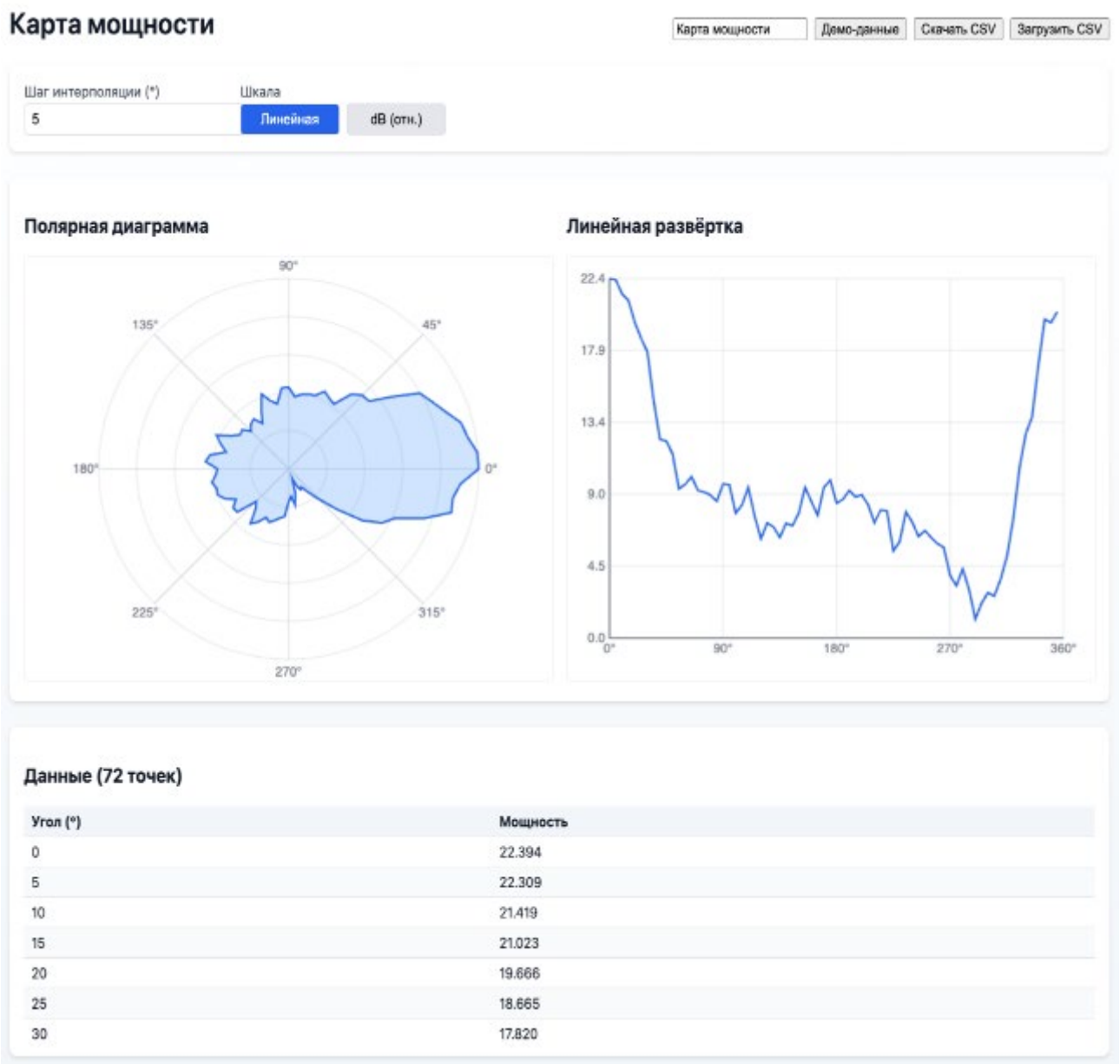

Рис. 3. Укрупненная визуализация карты мощности электромагнитного сигнала в полярной и декартовой системе координат

Это позволяет более точно определить вероятностную часть коррелограммы. Для решения проблемы повышения точности распознавания атаки Сибиллы с использованием коррелограммы необходимо применить методы машинного обучения, а именно, глубокие искусственные нейронные сети для идентификации карты мощности [9]. Также в составе робота-сервера должны быть предусмотрены дополнительные отсекатели электромагнитного

сигнала, предназначенные для формирования пространственно-неоднородного поля излучения.

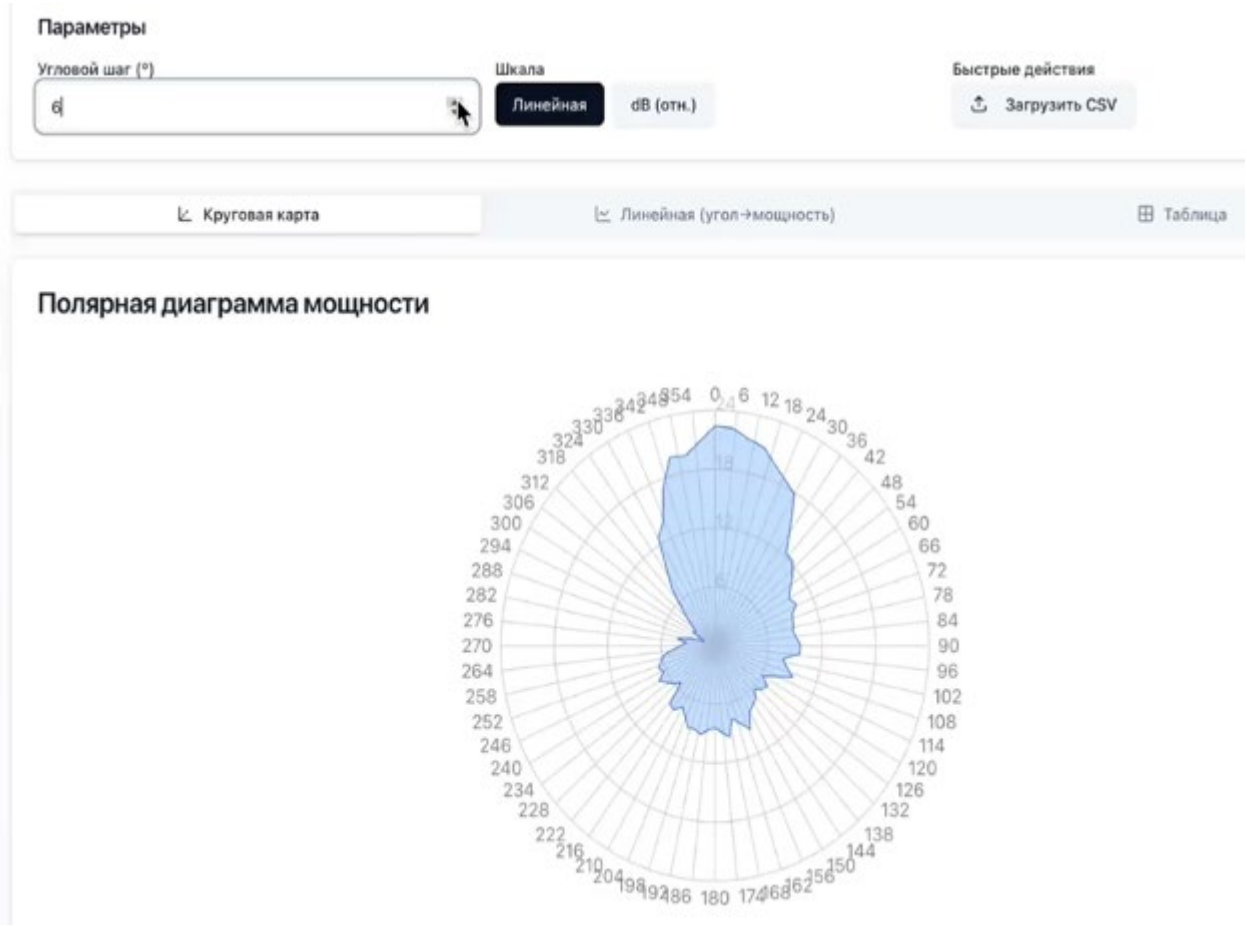

Рис. 4. Визуализация карты мощности электромагнитного сигнала в полярной системе координат

Это необходимо для того, чтобы карта мощности электромагнитного сигнала, измеренная на ровной поверхности при отсутствии статических и динамических препятствий, характеризовалась выраженной вариативностью значений, в том числе, наличием отчётливо различимых локальных максимумов и минимумов.

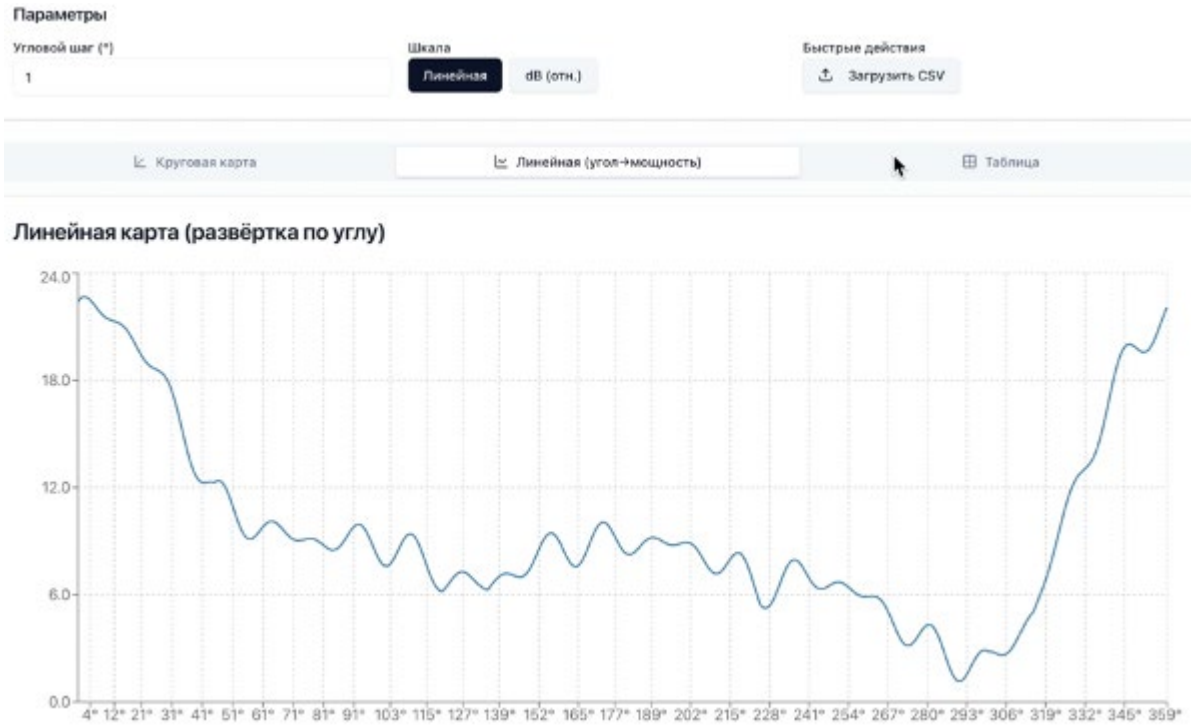

Рис. 4. Визуализация карты мощности электромагнитного сигнала в декартовой системе координат

Заключение

Представленный метод демонстрирует, что статистический анализ временных рядов сетевой активности, в частности построение и сравнение коррелограмм, является эффективным инструментом для выявления атаки Сибиллы с точностью от 83,2 % до 97,4 %. Метод основывается на фундаментальном ограничении атакующего — невозможности полностью эмулировать статистическую независимость сетевого поведения большого количества узлов, управляемых из одной точки. Данный вывод согласуется с результатами современных исследований, в которых показано, что коррелированные и структурно зависимые паттерны активности являются ключевым признаком Sybil-атак в распределённых системах [10], [11].

Преимуществами представленного метода являются:

1. Пассивность, т.е. отсутствие необходимости в создании дополнительной нагрузки на сеть, в отличие от методов, основанных на Proof-of-Work;
2. Низкая вычислительная стоимость, поскольку операции вычисления корреляционных функций являются относительно простыми;
3. Универсальность, заключающаяся в применимости метода к различным типам распределённых и P2P-систем;
4. Адаптивность, позволяющая выявлять атаки Сибиллы и другие формы вредоносной активности, маскирующиеся под легитимное сетевое поведение, что подтверждается современными обзорами методов противодействия подобным атакам [11].

В то же время были выявлены и ограничения предлагаемого подхода. Во-первых, для корректного выявления статистических зависимостей требуется достаточно продолжительный период наблюдения. Возможным решением данной проблемы является применение методов анализа в реальном времени на основе скользящего временного окна. Во-вторых, интеллектуальный злоумышленник может пытаться вносить случайные задержки в активность подконтрольных узлов. Для повышения устойчивости метода к подобным искажениям целесообразно использование алгоритмов динамического выравнивания временных рядов, таких как DTW. В-третьих, в отдельных случаях возможно совпадение легитимных паттернов сетевой активности, например у роботов-клиентов, находящихся в одной подсети. Снижение вероятности ложных срабатываний в таких ситуациях достигается за счёт комбинирования предложенного метода с дополнительными признаками, включая анализ IP-адресов и графов сетевой связности [12].

Дальнейшие исследования целесообразно направить на оптимизацию вычислительной сложности алгоритма, а также на интеграцию предложенного подхода с другими методами поведенческого анализа для

построения комплексных систем защиты распределённых систем. В частности, перспективным направлением является применение глубоких искусственных нейронных сетей для идентификации и классификации карт мощности электромагнитного сигнала роботов-клиентов, что позволит повысить точность и устойчивость обнаружения атак Сибиллы в сложных сетевых средах [10].

Литература

1. Варламов, Д. Л., Костров, В. В. Снижение уровня боковых лепестков корреляционной функции сложных дискретных сигналов при использовании мю-фильтрации // Методы и устройства передачи и обработки информации. – 2006. – № 7. – С. 116–121. – EDN NEJIAP.

2. Завгороднев, С. М., Коляда, А. А., Ревинский, В. В. Использование математического аппарата корреляционной функции для оптимизации гнездового алгоритма сравнения дактилоскопических изображений // Вопросы криминологии, криминалистики и судебной экспертизы. – 2013. – № 1(33). – С. 206–217. – EDN YUDOSF.

3. Чижма, С. Н., Газизов, Р. И. Использование корреляционных функций для спектрального анализа сигналов в системах электроснабжения // Динамика систем, механизмов и машин. – 2012. – № 1. – С. 292–295. – EDN SEOTCH.

4. Морозов, А. Н., Назолин, А. Л., Фуфурин, И. Л. Оптические и спектральные методы в задачах обнаружения и распознавания подвижных летательных объектов // Радиостроение. – 2020. – № 2. – С. 39–50. – DOI: 10.36027/rdeng.0220.0000167. – EDN QZVTAA.

5. Сюсюка, Е. Н., Хан, Д. А. Физико-математические основы спектрального анализа и его применение // Вестник государственного морского университета имени адмирала Ф. Ф. Ушакова. – 2019. – № 3(28). – С. 30–33. – EDN FBAPPU.

6. Иванов, Н. С. Помехоустойчивая М-оценка выборок многократных наблюдений // Метрология. – 2012. – № 9. – С. 3–14. – EDN PDTVCT.

7. Шевляков, Д. Г. Уменьшение уровня боковых лепестков по дальности в алгоритме вычисления прямой свёртки при совместном применении метода обратных пульсаций и сглаживании фронта сигнала // Радиопромышленность. – 2005. – № 1. – С. 131–145. – EDN HSAXSX.

8. Аксенов, А. В. Защита от атаки Сибиллы без использования распределения криптографических ключей // Инженерный вестник Дона. – 2025. – № 11. – URL: ivdon.ru/ru/magazine/archive/n11y2025/10500

9. Ерохин, В. В. Жадное послойное обучение сверточных нейронных сетей // Мягкие измерения и вычисления. – 2021. – Т. 48. – № 11. – С. 66–83. – DOI: 10.36871/2618-9976.2021.11.004. – URL: doi.org/10.36871/2618-9976.2021.11.004

10. Heeb, S., Plesner, A., Wattenhofer, R. Sybil detection using graph neural networks // arXiv. – 2024. – URL: arxiv.org/abs/2409.08631

11. Arshad, A., et al. A survey of Sybil attack countermeasures in IoT-based wireless sensor networks // PeerJ Computer Science. – 2021. – DOI: 10.7717/peerjcs.673.

12. Гавриков, М. М., Мезенцева, А. Ю. Использование метаграфов для описания семантики и прагматики информационных систем // Инженерный вестник Дона. – 2012. – № 4. – URL: ivdon.ru/ru/magazine/archive/n4p2y2012/1434

References

1. Varlamov D. L., Kostrov V. V. Metody i ustroistva peredachi i obrabotki informatsii, 2006, № 7, pp. 116–121.

2. Zavgorodnev S. M., Kolyada A. A., Revinskii V. V. Voprosy kriminologii kriminalistiki i sudebnoi ekspertizy, 2013, № 1(33), pp. 206–217.

3. Chizhma S. N., Gazizov R. I. Dinamika sistem mekhanizmov i mashin, 2012, № 1, pp. 292–295.

4. Morozov A. N., Nazolin A. L., Fufurin I. L. Radiostroenie, 2020, № 2, pp. 39–50. DOI: 10.36027/rdeng.0220.0000167.

5. Syusyuka E. N., Khan D. A. Vestnik gosudarstvennogo morskogo universiteta imeni admirala F. F. Ushakova, 2019, № 3(28), pp. 30–33.

6. Ivanov N. S. Metrologiya, 2012, № 9, pp. 3–14.

7. Shevlyakov D. G. Radiopromyshlennost', 2005, № 1, pp. 131–145.

8. Aksenov A. V. Inzhenernyj vestnik Dona, 2025, № 11. URL: ivdon.ru/ru/magazine/archive/n11y2025/10500

9. Erokhin V. V. Myagkie izmereniya i vychisleniya, 2021, vol. 48, № 11, pp. 66–83. DOI: 10.36871/2618-9976.2021.11.004. URL: doi.org/10.36871/2618-9976.2021.11.004

10. Heeb S., Plesner A., Wattenhofer R. arXiv, 2024. URL: arxiv.org/abs/2409.08631

11. Arshad A. et al. PeerJ Computer Science, 2021. DOI: 10.7717/peerjcs.673.

12. Gavrikov M. M., Mezentseva A. Yu. Inzhenernyj vestnik Dona, 2012, № 4. URL: ivdon.ru/ru/magazine/archive/n4p2y2012/1434

Дата поступления: 2.12.2025
Дата публикации: 6.02.2026