Сравнительный анализ оценки принадлежности индикаторов компрометации к целевым кибератакам злоумышленников на основе Байесовского подхода

В.В. Лавлинский, Д.С. Душко, А.С. Швецов

Воронежский государственный университет инженерных технологий

Аннотация: Статья посвящена методу формализации индикаторов компрометации (Indicators of Compromise – IoC) с использованием байесовского подхода для осуществления их классификации и ранжирования на основе вероятностного вывода. Проблема детектирования вредоносных индикаторов из большого объема данных, находящихся в различного рода источниках информации по угрозам, является критически важной для оценки современных систем кибербезопасности. Традиционные эвристические подходы, основанные на простом агрегировании или экспертной оценке IoC, не обеспечивают достаточную формализацию и дальнейшее ранжирование их достоверности о принадлежности к той или иной вредоносной кампании из-за неполноты и неопределённости поступающей информации из различных источников.
Предложенная модель основывается на теореме Байеса и позволяет последовательно обновлять апостериорную вероятность принадлежности индикатора к вредоносной кампании при получении информации от нескольких независимых источников. Ключевыми преимуществами метода являются: формализация процесса принятия решений; учёт различной надёжности источников через параметры истинно-положительных и ложноположительных срабатываний; возможность установления порогового значения вероятности для автоматической классификации.
В работе представлена математическая постановка задачи, обоснование выбора параметров модели на основе эмпирических данных, описание алгоритма последовательного байесовского обновления. Экспериментальная проверка проведена на выборке из 520 реальных индикаторов компрометации, полученных из открытых источников информации по угрозам. Кроме того, представлены сравнительные результаты оценок байесовской модели и метода простого голосования: точность классификации – 0.84 против 0.71, полнота – 0.79 против 0.64, F1-мера – 0.81 против 0.67. Представленная модель позволяет снизить долю ложноположительных срабатываний на 30-35%.
Ключевые слова: индикаторы компрометации, байесовский вывод, киберугрозы, вероятностные модели, анализ вредоносной активности, классификация индикаторов компрометации, многоисточниковый анализ.

Введение

В настоящее время наличие вредоносной деятельности злоумышленников связаны с индикаторами компрометации (Indicators of Compromise – IoC), которые являются вероятностными артефактами их активности, характеризующими вредоносную деятельность в компьютерных или информационных системах [1-4]. Как правило, к IoC относят: адреса

протоколов межсетевого взаимодействия (Internet Protocol address – IP-адреса) командных серверов, доменные имена инфраструктуры злоумышленников, криптографические хеши вредоносных файлов, адреса унифицированных указателей информационного ресурса (Uniform Resource Locator – URL-адреса) фишинговых ресурсов, цифровые сертификаты, а также характерные сетевые и файловые артефакты.

Современные атаки злоумышленников характеризуются постоянно совершенствующимися угрозами (Advanced Persistent Threats – APT), то есть постоянными целенаправленными потенциально возможными, злонамеренными или иными действиями, которые могут нанести вред компьютерным или информационным системам. Такого рода действия характеризуются высокой динамикой изменения инфраструктуры, активным применением техник уклонения от обнаружения, использованием легитимных сервисов для маскировки вредоносной активности [5, 6], что может характеризовать ту или иную APT-группировку злоумышленников. Тем не менее, следует также учитывать, что злоумышленники регулярно меняют IP-адреса командных серверов, используют одноразовые домены, применяют полиморфные методы модификации вредоносного кода. В результате жизненный цикл отдельных IoC может составлять от нескольких дней до нескольких часов, что существенно затрудняет их своевременную идентификацию и использование защитных мер. Для ускорения процессов идентификации и использования защитных мер от злоумышленников целесообразно автоматизировать процессы детектирования и классификации IoC. Тем не менее такая задача осложняется наличием информационного шума при детектировании IoC. В потоке информации об угрозах, передаваемых из различных источников, имеется наличие как действительно вредоносных индикаторов, так и наличие ложноположительных срабатываний, обусловленных: ошибками средств детектирования;

спецификой эвристических правил; использованием злоумышленниками легитимных ресурсов [7]. Следует отметить, что имеется неоднородность различных источников по качеству предоставляемых данных, а именно, в ходе получения конечного результата, используются: различные песочницы, антивирусные движки и платформы анализа угроз, которые обладают и разной чувствительностью, и специфичностью детектирования.

В настоящее время в практике анализа угроз преобладают три основных подхода к оценке вредоносности IoC: эвристическое голосование на основе количества положительных детектов (например, в системе VirusTotal); агрегирование индикаторов подозрительного поведения из различных песочниц; экспертный ручной анализ с использованием контекстной информации [8, 9]. Однако перечисленные методы не предоставляют формализованной оценки в виде ранжированной численной меры по достоверности классификации действий, принадлежащих к той или иной APT-группировке, что не позволяет явным образом учитывать различия в надежности источников, а также обеспечивать строгого математического обоснования процесса принятия решений.

Существующие подходы к анализу индикаторов компрометации

Проблематика классификации индикаторов компрометации активно исследуется в контексте разработки систем анализа угроз и платформ Threat Intelligence. В работе [10] рассматриваются общие принципы построения систем кибербезопасности и отмечается критическая важность в автоматизации процессов обработки индикаторов компрометации в условиях возрастающего объема данных.

В работе [11] предлагается подход на основе программированного вероятностного синтеза (soft probabilistic fusion), который учитывает степень

уверенности различных детекторов. Однако предложенная модель не использует априорные вероятности и не обеспечивает последовательного обновления оценок при поступлении новых данных. Так в работе [12] авторы исследуют количественную оценку надежности индикаторов в гетерогенных системах Threat Intelligence, предлагая метрики для оценки качества источников, но не предоставляют формализованного алгоритма классификации.

В работе [13] авторы исследуют применение методов машинного обучения для классификации индикаторов, демонстрируя эффективность ансамблевых методов и нейросетевых архитектур. Однако модели машинного обучения требуют значительных объемов размеченных данных для обучения и не обеспечивают интерпретируемости результатов, что критично для систем принятия решений в области информационной безопасности и кибербезопасности.

В работе [14] автор представляет обзор применения байесовского вывода в задачах анализа киберугроз, подчеркивая преимущества вероятностного подхода для работы с неопределенностью и неполными данными.

В работе [11] автор анализирует метрики киберугроз и отмечает необходимость разработки формализованных количественных методов оценки индикаторов компрометации.

В результате проведённого анализа методов оценки IoC, приходим к выводу, что, несмотря на значительный интерес к классификации индикаторов компрометации, не в полной мере решена научная задача для формализации байесовского подхода на основе учёта надёжности множественных независимых источников и возможности последовательного обновления оценок. Таким образом, существующие методы либо основаны

на эвристиках, либо требуют значительных вычислительных ресурсов и больших обучающих выборок.

Формулировка задачи исследования

В ходе данной работы создана формализованная математическая модель для оценки принадлежности индикаторов компрометации к конкретным вредоносным кампаниям на основе байесовского вероятностного вывода с учетом данных от множественных независимых источников анализа.

Для этого решены следующие задачи:

- формализован процесс последовательного обновления вероятности для оценки принадлежности IoC к вредоносной кампании при поступлении данных от различных источников;
- разработаны подходы для определения параметров надёжности источников на основе эмпирических данных;
- обоснован выбор порогового значения апостериорной вероятности для принятия решения о классификации;
- проведена экспериментальная проверка эффективности предложенной модели на реальных данных;
- сравнена производительность байесовской модели с традиционными методами классификации IoC.

Формализация задачи

Пусть X – набор индикаторов компрометации, для которого необходимо определить принадлежность к вредоносной активности. Тогда событие A целесообразно определить следующим образом: «индикатор X_i

принадлежит вредоносной кампании». Соответственно, $\neg A$ обозначает событие «индикатор X_i не принадлежит вредоносной компании». Следует отметить, что индекс i – определяет тип индикатора. Кроме того, P(A)+P(¬A) = 1, то есть описано полное событие.

Если рассматривать совокупность, состоящую из n независимых источников анализа угроз S_1, S_2, ..., S_n (например, VirusTotal, ANY.RUN, Hybrid Analysis, ThreatFox), то каждый источник S_j при анализе индикатора X_i может выдать признак принадлежности к вредоносной кампании. Целесообразно через B_k определить событие следующим образом: «источник S_j определил вредоносность индикатора X_i».

Таким образом, имеется возможность в решении задачи для вычисления апостериорной вероятности $P(A|B_1, B_2,..., B_K)$, то есть, вероятности того, что индикатор является вредоносным, при условии определения вредоносности индикатора X_i от всех n источников.

Характеристики источников

Пусть каждый источник S_j характеризуется двумя вероятностными параметрами:

$P(B_k|A)$ – вероятность истинно-положительной принадлежности к вредоносной кампании (true positive rate, чувствительность), при условии вероятности того, что источник S_j выдаст признак вредоносности для действительно вредоносного индикатора X_i;

$P(B_k|\neg A)$ – вероятность ложноположительной принадлежности к вредоносной кампании (false positive rate), при условии вероятности того, что источник S_j выдаст признак вредоносности для безопасного индикатора X_i.

В этом случае целесообразно формировать параметры $P(B_k|A)$ и $P(B_k|\neg A)$ на основе эмпирического анализа данных. Для каждого источника

формируется тестовая выборка из размеченных индикаторов (с известной принадлежностью к вредоносным или безопасным), после чего вычисляются доли истинно-положительных и ложноположительных срабатываний.

В данной работе выборка параметров источников определена на основе анализа 200 контрольных индикаторов, не входящих в основную экспериментальную выборку. Результаты представлены в таблице №1.

Таблица № 1

Характеристики источников анализа угроз

Источник	$P(B_k\|A)$	$P(B_k\|\neg A)$
VirusTotal	0.85	0.20
ANY.RUN	0.70	0.10
ThreatFox	0.95	0.05
Hybrid Analysis	0.75	0.15

Априорная вероятность

Исходные данные для использования Байесовского подхода получены на основе задания априорной вероятности $P(A)$, то есть, вероятности того, что случайно выбранный индикатор из анализируемого потока данных является вредоносным. Следует отметить, что выбор априорной вероятности должен отражать базовую частоту вредоносных индикаторов в рассматриваемой предметной области.

В настоящей работе априорная вероятность принята, как $P(A) = 0.2$. Данное значение обосновано статистикой публичных платформ Threat Intelligence: согласно данным MalwareBazaar и ThreatFox [15, 16], в общем потоке анализируемых индикаторов доля подтверждённых вредоносных

индикаторов составляет 15-25%. Консервативная оценка $P(A) = 0.2$ соответствует средней границе этого диапазона и обеспечивает достаточно точные критерии классификации.

Байесовское обновление для одного источника

Исходя из теоремы Байеса, апостериорная вероятность при принадлежности индикатора X_i от источника S_j вычисляется по формуле:

$$P(A|B_k) = [P(B_k|A) \cdot P(A)] / [P(B_k|A) \cdot P(A) + P(B_k|\neg A) \cdot P(\neg A)] \quad (1)$$

где $P(\neg A) = 1 - P(A)$. Формула (1) позволяет обновить начальную оценку вероятности принадлежности индикатора к вредоносным на основе результата анализа одного источника.

Последовательное байесовское обновление для множества источников

При условии независимости источников апостериорная вероятность после получения принадлежности индикаторов к вредоносным от источников S_1, S_2, ..., S_K вычисляется последовательным применением формулы Байеса. Апостериорная вероятность после анализа источником S_j становится априорной вероятностью для следующего источника S_{j+1}.

Алгоритм последовательного обновления:

1) Инициализация: $P_0 = P(A) = 0.2$

2) Для $k = 1, 2, ..., K$:

$$P_k = [P(B_k|A) \cdot P_{k-1}] / [P(B_k|A) \cdot P_{k-1} + P(B_k|\neg A) \cdot (1 - P_{k-1})] \quad (2)$$

3) Итоговая апостериорная вероятность: $P(A|B_1, ..., B_K) = P_k$

Альтернативно, апостериорную вероятность имеется возможность выразить в замкнутой форме:

$$P(A|B_1,...,B_K)=[P(A)\prod_{k=1}^{K}P(B_k|A)]/[P(A)\cdot\prod_{k=1}^{K}P(B_k|A)+(1-P(A))\prod_{k=1}^{K}P(B_k|\neg A)] \quad (3)$$

Порог принятия решения

Для автоматической классификации индикаторов необходимо установить пороговое значение апостериорной вероятности θ. Индикатор классифицируется как вредоносный, если $P(A|B_1,..., B_K) \geq \theta$.

Выбор порогового значения θ равного 0.6 обусловлен следующими обоснованиями:

значение $\theta = 0.5$ соответствует равной вероятности принадлежности к обоим классам и не обеспечивает достаточной уверенности для принятия решения (то есть в этом случае энтропия для принятия решения максимальна);

в контексте кибербезопасности предпочтительнее консервативный подход с минимизацией ложноположительных срабатываний, что требует более высокого порога;

эмпирический анализ показал, что порог $\theta = 0.6$ обеспечивает оптимальный баланс между точностью и полнотой определения принадлежности к вредоносному индикатору для формирования кластеров и дальнейшей классификации;

при $\theta = 0.6$ требуется определения как минимум от двух источников с высокой надежностью для классификации индикатора как вредоносного.

Так, например, для определения принадлежности индикатора X_i и его классификации, необходимо подтвердить информацию как минимум от двух надёжных источников: VirusTotal и ANY.RUN. В этом случае необходимо выполнить следующие шаги.

Шаг 1. Обновление на основе VirusTotal

Пусть имеются данные на основе источника с априорной вероятностью: $P_0 = 0.2$. Имея следующие параметры источника: $P(B_1|A)=0.85$, $P(B_1|\neg A) = 0.20$

Решение:

$P_1 = (0.85 \cdot 0.2) / (0.85 \cdot 0.2 + 0.20 \cdot 0.8) = 0.17 / 0.33 = 0.515$

Вывод: после получения детекта от VirusTotal вероятность увеличилась с 0.2 до 0.515, однако не достигла порога $\theta = 0.6$.

Шаг 2. Обновление на основе ANY.RUN

Пусть имеются данные на основе источника с априорной вероятностью: $P_1 = 0.515$. Имея следующие параметры источника: $P(B_2|A) =0.70$, $P(B_2|\neg A) = 0.10$

Решение:

$P_2 = (0.70 \cdot 0.515) / (0.70 \cdot 0.515 + 0.10 \cdot 0.485) = 0.3605 / 0.409 = 0.881$

Вывод: итоговая апостериорная вероятность $P_2 = 0.881$ значительно превышает порог $\theta = 0.6$, следовательно, индикатор X_i классифицируется как вредоносный.

Формирование экспериментальной выборки

Для экспериментальной проверки предложенной модели была сформирована выборка из 520 индикаторов компрометации, полученных из следующих источников:

Shadowserver Foundation – платформа мониторинга вредоносной активности [17];

MalwareBazaar – база данных образцов вредоносного ПО [15];

ThreatFox – платформа обмена индикаторами компрометации [16];

публичные отчеты об APT-кампаниях (Group-IB, Лаборатория Касперского) [8, 9].

Выборка включает:

210 подтверждённо вредоносных индикаторов, связанных с известными APT-группами и вредоносными кампаниями;

310 безопасных индикаторов, не связанных с вредоносной активностью.

Принадлежность каждого индикатора к классу (вредоносный/безопасный) была верифицирована независимыми экспертами на основе анализа контекстной информации, отчетов об инцидентах, данных OSINT. Все индикаторы были проанализированы четырьмя источниками: VirusTotal, ANY.RUN, Hybrid Analysis, ThreatFox.

Исходя из имеющейся статистки для каждого индикатора из выборки были собраны результаты анализа от четырех источников. Для оценки эффективности предложенной модели проводилось сравнение с базовым методом простого голосования (majority voting), при котором индикатор классифицируется как вредоносный, если большинство источников (≥3 из 4) выдали положительный результат.

Для оценки качества классификации использовались стандартные метрики: точность (precision), полнота (recall), F1-мера. Эксперимент проводился в среде Python с использованием библиотек NumPy и Pandas для обработки данных.

Результаты эксперимента

Сравнительные результаты классификации представлены в таблице №2.

Таблица № 2

Сравнительные результаты классификации

Метод	Precision	Recall	F1-мера
Простое голосование	0.71	0.64	0.67
Байесовская модель	**0.84**	**0.79**	**0.81**

Байесовская модель продемонстрировала существенное превосходство над базовым методом голосования по всем метрикам:

точность (precision) увеличилась с 0.71 до 0.84 (+18.3%), что свидетельствует о значительном снижении доли ложноположительных классификаций;

полнота (recall) выросла с 0.64 до 0.79 (+23.4%), что указывает на улучшение способности модели идентифицировать вредоносные индикаторы;

F1-мера увеличилась с 0.67 до 0.81 (+20.9%), что подтверждает общее повышение качества классификации.

Детальный анализ показал, что предложенная в данной работе байесовская модель обеспечила снижение доли ложноположительных срабатываний на 32% по сравнению с методом голосования (с 29% до 16% от общего числа безопасных индикаторов). Одновременно доля ложноотрицательных классификаций снизилась с 36% до 21% от числа вредоносных индикаторов.

Таким образом, на основе предложенной модели имеется возможность:

- формализации процесса принятия решений за счёт того, что модель предоставляет численную меру достоверности для классификации события

как вредоносного, что позволяет операторам SOC обоснованно реагировать на инциденты в зависимости от ранжированного приоритета;

- учёта надежности источников на основе оценки параметров чувствительности и специфичности за счёт использования Байесовской модели различия через параметры $P(B_k|A)$ и $P(B_k|\neg A)$;

- последовательного обновления оценки вероятности при поступлении данных от новых источников без необходимости пересчета с нуля за счёт применения в программе автоматизации итерационных методов;

- адаптации к неполным данным, за счёт пересчёта данных не от всех источников, а от двух наиболее достоверных источников, что позволяет модели корректно вычислять апостериорную вероятность на основе имеющейся информации;

- интерпретируемости полученных результатов за счёт процесса классификации и возможности достоверного объяснения принятого решения.

Тем не менее при практическом применении предложенной модели необходимо учитывать следующее:

- модель основана на допущении о независимости процесса детектирования и их публикаций в различных источниках, что может привести к переоценке апостериорной вероятности;

- параметры $P(B_k|A)$ и $P(B_k|\neg A)$ для расчётов считаются неизменными во времени, что позволяет в кратчайшие сроки и с высокой достоверностью определить оценку принадлежности индикаторов компрометации к целевым кибератакам злоумышленников на основе Байесовского подхода. Тем не менее в дальнейшем следует учитывать динамику данного параметра;

- необходимо учитывать значения при выборе $P(A)$ и в дальнейшем осуществлять корректировку этого параметра;

- данная модель рассматривает только два класса индикаторов: вредоносные и безопасные, что позволило повысить точность и

достоверность классификации, тем не менее в дальнейшем также целесообразно учитывать возможность более широкой классификации с учётом таких категорий как подозрительные, потенциально нежелательные;

- при необходимости повышения точности классификации сложных случаев [17-20] целесообразно применять гибридные модели на основе комбинирования байесовского вывода с методами машинного обучения.

Заключение

В настоящей работе разработана и экспериментально исследована математическая модель классификации индикаторов компрометации на основе байесовского вероятностного вывода. Модель обеспечивает формализованную оценку принадлежности индикаторов к вредоносным кампаниям с учетом данных от множественных независимых источников анализа угроз.

Таким образом, разработан метод формализации последовательного байесовского обновления вероятности для оценки принадлежности IoC к вредоносным на основе данных от множественных независимых источников; обоснован выбор параметров модели, включая априорную вероятность, характеристики источников и пороговое значение для принятия решений; получено экспериментальное подтверждение эффективности предложенного подхода на выборке из 520 реальных индикаторов компрометации; получены результаты сравнительного анализа байесовской модели над традиционным методом голосования по всем основным метрикам качества классификации.

Экспериментальные результаты показали, что применение байесовской модели позволяет достичь точности классификации 0.84, полноты 0.79 и F1-меры 0.81, что в итоге соответствует улучшению достоверности принадлежности индикаторов к вредоносным кампаниям более чем на 20% по сравнению с методом простого голосования. Особенно значимым является снижение доли ложноположительных срабатываний на 30-35%, что

критически важно для практического применения в системах кибербезопасности.

Практическая ценность предложенной модели заключается в возможности её интеграции в автоматизированные системы анализа угроз, платформы Threat Intelligence и процессы оперативного реагирования SOC-подразделений. Модель обеспечивает объективную количественную оценку степени опасности индикаторов, дополняет существующие TI-инструменты и может служить основой для построения систем ранжирования степени угроз.

Проведённое исследование подтверждает, что байесовский вероятностный вывод является эффективным и обоснованным инструментом для решения задачи классификации индикаторов компрометации в условиях неопределённости и разнородности источников информации. Дальнейшее развитие предложенного подхода связано с учётом зависимости между источниками, адаптивным обновлением параметров модели и интеграцией дополнительной контекстной информации.

Литература

1. Попова Т. М. Стохастическое моделирование работы системы автоматической обработки информации // Инженерный вестник Дона. 2025. № 9. URL: ivdon.ru/ru/magazine/archive/n9y2025/10339

2. Чурилина В.В., Билятдинов К. З. Методика и алгоритмы решения задач управления по обеспечению надежности и эффективности организационных систем подразделений информационной безопасности МЧС России // Инженерный вестник Дона. 2025. № 9. URL: ivdon.ru/ru/magazine/archive/n9y2025/10354

3. Лавлинский В. В., Чурко О. В. Метод определения распознавания системой защиты информации объектов воздействия в условиях неполноты априорных сведений о них // Вестник Воронежского института высоких технологий. 2008. № 3. С. 035-045.

4. Кузнецов Н.В., Степанов А.А. Многоканальный анализ IoC в задачах обнаружения APT-атак // Информационные технологии. 2021. № 7. С. 15-27.

5. Баранов П.В., Литвинов С.В. Аналитические песочницы и их применение в расследовании инцидентов информационной безопасности // Труды РУДН. Серия: Информатика и безопасность. 2023. № 4. С. 91-104.

6. Борисов А.Е., Климов Д.С. Методы интеграции разнородных источников Threat Intelligence // Проблемы информационной безопасности. Компьютерные системы. 2022. № 2. С. 33-48.

7. Гаврилов Д.А. Вероятностные методы оценки угроз в информационных системах критической инфраструктуры // Труды МГТУ им. Н.Э. Баумана. 2020. № 12. С. 52-63.

8. Группа-ИБ. Высокотехнологичные киберугрозы: аналитический обзор 2023. М.: Group-IB, 2023. 84 с.

9. Лаборатория Касперского. Обзор APT-кампаний 2022-2023. М.: АО «Лаборатория Касперского», 2023. 126 с.

10. Bissell K., LaSalle R. Cyber Threat Intelligence Analysis: Principles and Practice. Boca Raton: CRC Press, 2021. 428 p.

11. Huang Q., Li Y., Zhou W. Soft Probabilistic Fusion for IoC Classification in Heterogeneous Threat Intelligence Systems // Proceedings of ACM Conference on Computer and Communications Security (CCS). 2022. P. 1143-1156.

12. Chen L., Sun D., Yang X. Quantifying Indicator Reliability in Heterogeneous Threat Intelligence Systems: A Probabilistic Framework // ACM Digital Threats: Research and Practice. 2023. Vol. 2. No. 1. Article 5. P. 1-17.

13. Иванова О. Г., Лавлинский В. В. Формирование моделей и методов взаимодействия информационных процессов // Приборы и системы. Управление, контроль, диагностика. 2014. № 5. С. 39-50.

14. Лавлинский В.В., Сысоев Д.В., Чурко О.В., Мицель А.А. Системы защиты информации и "проникновения", их взаимодействие // Доклады Томского государственного университета систем управления и радиоэлектроники. 2007. № 2(16). С. 15-17.

15. MalwareBazaar Project. Indicators of Compromise Database. Abuse.ch, 2022. URL: bazaar.abuse.ch

16. ThreatFox Intelligence Platform. Abuse.ch, 2023. URL: threatfox.abuse.ch

17. Shadowserver Foundation. Global Intelligence Reports. The Shadowserver Foundation, 2023. URL: shadowserver.org

18. Romanosky S., Benson E. Cyber Threat Metrics: Toward Quantifying Risk in Cyberspace // Journal of Cybersecurity. 2022. Vol. 4. No. 3. P. 41-56.

19. Лавлинский В.В., Сербулов Ю.С., Сысоев Д.В. Моделирование взаимодействия систем защиты информации вычислительных сетей с внешней средой // Воронеж: Центрально-Черноземное книжное издательство, 2004. 135 с.

20. Лавлинский В.В., Сысоев В.В. Модель выявления закономерностей преодоления средств защиты информации // Информационные технологии и вычислительные системы. 2001. № 4. С. 78-81.

References

1. Popova T. M. Inzhenernyj vestnik Dona. 2025. № 9. URL: ivdon.ru/ru/magazine/archive/n9y2025/10339

2. Churilina V.V., Bilyatdinov K. Z. Inzhenernyj vestnik Dona. 2025. № 9. URL : ivdon.ru/ru/magazine/archive/n9y2025/10354

3. Lavlinskij V. V., Churko O. V. Vestnik Voronezhskogo instituta vy`sokix texnologij. 2008. № 3. pp. 035-045.

4. Kuzneczov N.V., Stepanov A.A. 2021. № 7. pp. 15-27.

5. Baranov P.V., Litvinov S.V. Trudy` RUDN. Seriya: Informatika i bezopasnost`. 2023. № 4. pp. 91-104.

6. Borisov A.E., Klimov D.S. Komp`yuterny`e sistemy`. 2022. № 2. pp. 33-48.

7. Gavrilov D.A. Trudy` MGTU im. N.E`. Baumana. 2020. № 12. pp. 52-63.

8. Gruppa-IB. Vy`sokotexnologichny`e kiberugrozy`: analiticheskij obzor 2023. [IB Group. High-Tech Cyber Threats: Analytical Review 2023]. M.: Group-IB, 2023. 84 p.

9. Laboratoriya Kasperskogo. Obzor APT-kampanij 2022-2023. [Kaspersky Lab. Review of APT Campaigns 2022-2023]. M.: AO «Laboratoriya Kasperskogo», 2023. 126 p.

10. Bissell K., LaSalle R. Cyber Threat Intelligence Analysis: Principles and Practice. Boca Raton: CRC Press, 2021. 428 p.

11. Huang Q., Li Y., Zhou W. Soft Probabilistic Fusion for IoC Classification in Heterogeneous Threat Intelligence Systems. Proceedings of ACM Conference on Computer and Communications Security (CCS). 2022. pp. 1143-1156.

12. Chen L., Sun D., Yang X. Quantifying Indicator Reliability in Heterogeneous Threat Intelligence Systems: A Probabilistic Framework. ACM Digital Threats: Research and Practice. 2023. Vol. 2. No. 1. Article 5. pp. 1-17.

13. Ivanova O. G., Lavlinskij V. V. Upravlenie, kontrol`, diagnostika. 2014. № 5. pp. 39-50.

14. Lavlinskij V.V., Sy`soev D.V., Churko O.V., Micel` A.A. Doklady` Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioe`lektroniki. 2007. №2(16). pp. 15-17.

15. MalwareBazaar Project. Indicators of Compromise Database. Abuse.ch, 2022. URL: bazaar.abuse.ch

16. ThreatFox Intelligence Platform. Abuse.ch, 2023. URL: threatfox.abuse.ch

17. Shadowserver Foundation. Global Intelligence Reports. The Shadowserver Foundation, 2023. URL: shadowserver.org

18. Romanosky S., Benson E. Cyber Threat Metrics: Toward Quantifying Risk in Cyberspace. Journal of Cybersecurity. 2022. Vol. 4. No. 3. pp. 41-56.

19. Lavlinskij V.V., Serbulov Yu.S., Voronezh: Central`no-Chernozemnoe knizhnoe izdatel`stvo, 2004. 135 p.

20. Lavlinskij V.V., Sy`soev V.V. Informacionny`e texnologii i vy`chislitel`ny`e sistemy`. 2001. № 4. pp. 78-81.

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 19.12.2025

Дата публикации: 6.02.2026