УДК 004.051

МЕТОДИКА ФОРМИРОВАНИЯ ПРОФИЛЕЙ УЯЗВИМОСТИ ОБЪЕКТОВ ЗАЩИТЫ НА БАЗЕ РЕТРОСПЕКТИВНЫХ ДАННЫХ

Саитов И.А., Кунин Н.Т.

Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет», Москва, Россия, saitov_i@mirea.ru

Аннотация: обеспечение предиктивной кибербезопасности современных программно-аппаратных объектов защиты требует перехода от качественных оценок угроз к строгим количественным моделям. Актуальной научно-технической задачей параметризации таких моделей является определение статистических вероятностей и ожидаемого ущерба от будущих кибератак. В данной статье предлагается комплексная методика формирования «профилей уязвимостей» на основе интеллектуального анализа ретроспективных данных из глобальных и национальных баз. Основной фокус работы направлен на способы сбора, очистки и статистической кластеризации накопленных массивов данных об уязвимостях. В исследовании описывается алгоритм трансляции разрозненных метрик в стандартизированные векторы, а также применение методов машинного обучения для группировки сотен тысяч инцидентов в ограниченный набор типизированных профилей. Для каждого сформированного профиля вычисляется статистическая вероятность возникновения в заданном стеке технологий и ожидаемый вес тяжести последствий. Результаты применения предложенного инструментария профилирования предоставляют исследователям и системным архитекторам достоверные эмпирические данные, которые могут быть напрямую использованы в качестве входных параметров для стохастических риск-моделей, расчета барьерных функций надежности и автоматизации предиктивного патч-менеджмента.

Ключевые слова: предиктивная безопасность, профиль уязвимости, ретроспективный анализ, интеллектуальный анализ данных, кластеризация угроз, базы данных уязвимостей, статистическая оценка вероятности.

ВВЕДЕНИЕ

Современный ландшафт кибернетических угроз характеризуется не только беспрецедентным ростом числа атак, но и непрерывным усложнением программно-аппаратных архитектур объектов защиты. Повсеместное внедрение автономных интеллектуальных агентов, систем Интернета вещей и облачных вычислений многократно расширило поверхность атаки. В этих условиях традиционные реактивные (апостериорные) подходы к информационной безопасности, основанные на устранении уязвимостей уже после их обнаружения и публикации, демонстрируют свою ограниченность. Обеспечение устойчивости критически важных систем требует перехода к парадигме предиктивной кибербезопасности, ядром которой являются строгие математические модели оценки рисков, в том числе стохастические.

Фундаментальной проблемой параметризации любых предиктивных математических моделей является высокая степень неопределенности. Предсказать точное время появления конкретной уязвимости «нулевого дня» в определенном программном модуле, а также вычислить точный вектор ее эксплуатации невозможно. Эти события носят выраженный случайный характер. Тем не менее сами процессы выявления уязвимостей подчиняются глобальным статистическим законам. Опираясь на закон больших чисел, можно выдвинуть гипотезу: хотя предсказать единичную «0-*day*»-угрозу нельзя, статистическое поведение целых классов (профилей) уязвимостей для конкретных стеков технологий поддается достоверному прогнозированию.

За последние два десятилетия мировым ИТ-сообществом накоплен колоссальный объем информации об инцидентах безопасности. Глобальные и национальные базы данных, такие как Национальная база данных уязвимостей США (*NVD*), реестр *MITRE CVE*, а также Банк данных угроз безопасности информации (БДУ) ФСТЭК России, содержат сотни тысяч записей. Тем не менее, эти массивы представляют собой «сырые», зачастую неструктурированные и гетерогенные данные. Использование устаревших метрик оценки, неполнота векторов (например, по стандарту *CVSS*) и преобладание текстовых описаний над формализованными атрибутами делают невозможным их прямое использование в качестве входных переменных для инженерных расчетов и математического моделирования устойчивости киберфизических систем. Существует критический разрыв между накопленным объемом исторических логов и возможностью их алгоритмического применения в риск-ориентированных моделях объектов защиты.

Целью данной статьи является разработка нового подхода и описание комплексной методики формирования формализованных «профилей уязвимостей» на основе интеллектуального анализа ретроспективных данных. Предлагаемый инструментарий направлен на решение задачи автоматизированного сбора, нормализации и статистической кластеризации массивов информации о киберугрозах. Результатом применения разработанного научно-методического аппарата будет являться перевод разрозненных исторических инцидентов в ограниченный набор структурированных математических профилей, описываемых вероятностными и весовыми характеристиками. Это позволит сформировать достоверный эмпирический фундамент для параметризации предиктивных систем защиты информации.

ОПИСАНИЕ КОМПЛЕКСНОЙ МЕТОДИКИ

Фундаментом для построения объективных статистических профилей уязвимостей является репрезентативная и постоянно обновляемая источниковая база. В современной практике информационной безопасности накоплен значительный массив данных об инцидентах и программных закладках. В качестве основных доноров для формирования обучающих датасетов выступают:

1. Глобальные реестры. Национальная база данных уязвимостей США (*NVD*), поддерживаемая *NIST*, и реестр *CVE* (*Common Vulnerabilities and Exposures*) корпорации *MITRE*. Они предоставляют наиболее массовую выгрузку, содержащую сотни тысяч записей, начиная с конца 1990-х годов.
2. Национальные базы данных. Банк данных угроз безопасности информации (БДУ) ФСТЭК России. Использование БДУ критически важно для профилирования систем, функционирующих в отечественном правовом поле, так как он содержит специфичную привязку к архитектурам сертифицированных средств защиты и отечественным ОС (например, семейства *Linux*).
3. Реестры эксплойтов и практической эксплуатации. Базы данных, такие как *Exploit-DB* или каталог *CISA KEV* (*Known Exploited Vulnerabilities*), которые предоставляют маркеры фактической (а не только теоретической) эксплуатируемости уязвимости.

Автоматизированный сбор информации (агрегация) осуществляется посредством *REST API*-интерфейсов и парсинга *JSON*-выгрузок, что позволяет сформировать первичное «озеро данных» (*Data Lake*). Однако прямое использование полученного агрегированного датасета для параметризации математических моделей невозможно. На этапе сбора исследователи сталкиваются с выраженной проблемой «грязных» (неполных и противоречивых) и гетерогенных данных.

Можно выделить три фундаментальные проблемы, требующие применения алгоритмов очистки и нормализации:

- Проблема неполноты и гетерогенности метрических векторов. Исторические записи в базах данных оценивались по разным стандартам. Уязвимости, обнаруженные до 2015 года, имеют векторы по стандарту *CVSS v*2.0; более поздние - по *CVSS v*3.0 и *v*3.1. Для корректной оценки деградации барьерных функций киберфизических и *IoT*-систем требуется использование метрик современного стандарта *CVSS* 4.0. Возникает несоответствие - большинство ретроспективных записей физически не имеют этих параметров.
- Проблема неструктурированного текста. Наиболее ценная архитектурная информация (причина возникновения ошибки, тип затронутого модуля, характер последствий) чаще всего содержится в поле description в виде произвольного текста на естественном языке. В сыром виде эти данные недоступны для алгоритмов кластеризации, оперирующих векторными пространствами.
- Проблема дублирования и противоречивости. При слиянии выгрузок из *NVD* и БДУ ФСТЭК часто возникают коллизии, при которых одна и та же уязвимость может иметь различающиеся оценки тяжести или векторы в разных базах из-за разницы в методологиях экспертной оценки.

Для решения описанных проблем перед этапом интеллектуального анализа вводится обязательный конвейер нормализации датасета. Предлагаемый алгоритм нормализации включает следующие шаги:

1. Дедупликация и кросс-валидация. Слияние записей из разных баз данных по ключу (*CVE ID*) с разрешением конфликтов в пользу более современных или национальных стандартов (например, приоритизация вектора из БДУ для отечественного ПО).
2. Эвристический маппинг векторов. Применение эвристических правил для трансляции базовых метрик *CVSS* v3.1 в приближенные эквиваленты *CVSS* 4.0. Например, если в *CVSS v*3.1 параметр Scope имел значение Changed (C), алгоритм автоматически проецирует это на высокие показатели *Subsequent System* (*S*) в *CVSS* 4.0.
3. Токенизация и фильтрация. Подготовка текстовых описаний к машинному анализу.

В результате выполнения процедур "очистки" формируется нормализованный реляционный датасет, в котором каждая строка представляет собой вектор-запись, очищенную от информационного шума и готовую к применению алгоритмов *Data Mining* и машинного обучения.

После завершения этапа сбора и нормализации ретроспективный массив данных представляет собой реляционную структуру, содержащую сотни тысяч записей об уникальных инцидентах. Каждая запись содержит как формализованные категориальные атрибуты, так и неструктурированный текст на естественном языке, такой как описания архитектурных причин и последствий уязвимостей.

Использование каждой отдельной исторической записи в качестве независимой переменной для математического моделирования надежности вычислительно нецелесообразно и не имеет статистического смысла. Для построения достоверных риск-моделей необходим переход от единичных инцидентов (микроуровень) к обобщенным типизированным классам угроз (макроуровень). Данная задача решается посредством применения методологии интеллектуального анализа данных и алгоритмов машинного обучения без учителя.

Предлагаемый в разрабатываемой методике процесс выявления профилей уязвимостей алгоритмически разделяется на три взаимосвязанных этапа.

Первым этапом выступает векторизация неструктурированного текста. Наибольшая информационная ценность о физическом смысле уязвимости заложена в текстовом поле её описания (*description*). Для того чтобы алгоритмы машинного обучения могли анализировать семантическую близость различных киберугроз, текст необходимо перевести в математическое представление. Для решения этой задачи применяются методы обработки естественного языка (*Natural Language Processing, NLP*). В простейшем случае используется мера *TF-IDF* (*Term Frequency - Inverse Document Frequency*), позволяющая выделить наиболее значимые архитектурные термины (например, «*buffer overflow*», «*SQL injection*», «*hardcoded credentials*»). В более продвинутых реализациях метода применяются плотные векторные представления (*Word Embeddings*) на базе нейросетевых архитектур класса *Transformer* (например, модели семейства *BERT*, дообученные на корпусах текстов по кибербезопасности). В результате каждое текстовое описание транслируется в числовой вектор фиксированной размерности, отражающий семантическую суть уязвимости.

Второй этап – построение единого многомерного признакового пространства. Полученные на предыдущем шаге текстовые векторы (отражающие причину ошибки) конкатенируются с нормализованными векторами метрик *CVSS* (отражающими сложность эксплуатации и тяжесть последствий). Образуется единое многомерное пространство признаков. В этом пространстве каждая уязвимость представляет собой точку. Уязвимости, имеющие схожие архитектурные причины, требующие одинаковых привилегий для эксплуатации и вызывающие сопоставимый ущерб, будут располагаться в этом пространстве близко друг к другу.

Заключительным, третьим этапом является алгоритмическая кластеризация. Для автоматического выявления плотных скоплений точек в сформированном многомерном пространстве применяются алгоритмы кластеризации. В контексте анализа баз данных уязвимостей высокую эффективность демонстрируют алгоритмы, основанные на плотности, такие как *DBSCAN* (*Density-Based Spatial Clustering of Applications with Noise*) или *HDBSCAN*.

Выбор плотностных алгоритмов обусловлен их способностью находить кластеры произвольной формы и автоматически отфильтровывать статистический шум (аномальные или единичные, нетипичные уязвимости, которые не должны искажать глобальную статистику). В качестве альтернативы, при необходимости задать жесткое количество искомых профилей, может применяться алгоритм K-Means с предварительным снижением размерности методами *PCA* или *t-SNE*.

В результате выполнения процедуры кластеризации исходный массив из сотен тысяч разрозненных *CVE* разбивается на ограниченное число непересекающихся групп. Каждый сформированный кластер C_j математически описывается своим «центроидом» – усредненным вектором признаков, отражающим наиболее типичные характеристики всех вошедших в него уязвимостей.

Именно этот центроид кластера, дополненный списком наиболее частотных семантических маркеров (ключевых слов) и усредненным вектором *CVSS*, в рамках предлагаемого подхода формализуется как «профиль уязвимости». Данный профиль становится строго параметризованным объектом, готовым к дальнейшим вероятностным расчетам.

Выделенные на этапе алгоритмической кластеризации плотные скопления инцидентов представляют собой семантически и метрически однородные группы киберугроз. Однако для использования этих данных в инженерных расчетах и предиктивной аналитике требуется строгая математическая формализация. Каждый кластер C_j (где $j = 1, 2, \dots, N$) трансформируется в эталонный «профиль уязвимости» путем вычисления двух ключевых количественных характеристик: статистической вероятности возникновения и усредненного веса тяжести последствий.

Важно отметить, что формирование профилей осуществляется не для всего глобального массива данных, а таргетированно – для конкретных стеков технологий S. Это обусловлено тем, что ландшафт угроз для облачного сервера и полевого сенсора принципиально различен.

Вероятность появления конкретного профиля уязвимости в заданном стеке технологий вычисляется на основе ретроспективной частоты. На базе закона больших чисел мы принимаем историческую частоту за статистическую вероятность будущего события.
Для заданного анализируемого стека S вероятность *j*-го профиля вычисляется по формуле:

$$p_j = \frac{n_j}{N_{total}},$$

где n_j – количество уязвимостей, принадлежащих кластеру C_j, которые затрагивают программные компоненты целевого стека S; N_{total} – общее количество уязвимостей в целевом стеке S, обнаруженных за репрезентативный ретроспективный период (например, за последние 5 лет).

При этом должно строго выполняться условие нормировки: сумма вероятностей всех выделенных профилей для конкретного стека равна единице ($\sum_{j=1}^{N} p_j = 1$). Данный показатель p_j отражает стохастическую предрасположенность выбранной архитектуры к уязвимостям определенного класса.
Вторым фундаментальным параметром профиля является его потенциальный разрушительный потенциал (вес). Так как каждый кластер содержит множество близких, но не идентичных уязвимостей, вес профиля вычисляется как усредненное значение нормализованных метрик тяжести всех вошедших в него инцидентов. В контексте современных подходов к оценке безопасности целесообразно использовать метрики стандарта *CVSS* 4.0. Для каждой уязвимости i внутри кластера вычисляется скалярный вес $w_i \in [0; 1]$. Способ конвертации метрик *CVSS* в скалярный вес зависит от предметной области. Например, для сегмента киберфизических систем наивысший приоритет получают профили, нарушающие метрики доступности уязвимой (*VA*) и последующих систем (*SA*), а также не поддающиеся автоматическому восстановлению (*Recovery*). Усредненный вес профиля вычисляется как среднее арифметическое (или медианное значение для исключения влияния статистических выбросов внутри кластера):

$$W_j = \frac{1}{n_j}\sum_{i=1}^{n_j} w_i.$$

Синтезируя результаты анализа текста, метрической кластеризации и статистических расчетов, мы можем формально определить «Профиль уязвимости» (PF_j) как упорядоченный кортеж:

$$PF_j = \langle K_j, \overline{V}_j, p_j, W_j \rangle,$$

где K_j – вектор ключевых семантических маркеров, извлеченный центроид кластера на этапе *NLP*; $\overline{V}_j$ – усредненный категориальный вектор метрик *CVSS* (наиболее типичный сценарий эксплуатации); p_j – вычисленная статистическая вероятность возникновения; W_j – вычисленный ожидаемый вес тяжести последствий.

Именно этот формализованный набор параметров делает профиль уязвимости самодостаточным, отчуждаемым и переиспользуемым объектом. Он позволяет исследователям оперировать не хаотичным потоком ежедневных отчетов об ошибках, а конечным набором типизированных математических сущностей, описывающих глобальные тренды безопасности для выбранной архитектуры объекта защиты.
Научная новизна представленного подхода состоит в формировании на основе гетерогенных ретроспективных данных достоверных оценок вероятности появления конкретного профиля уязвимости и его потенциального разрушительного потенциала в заданном стеке технологий, применяемых на объекте защиты. В условиях недостаточной оперативности существующих способов реактивной аналитики угроз такие научно-методические инструменты способствуют проактивному инженерному проектированию объектов защиты. Полученный набор формализованных профилей выступает в качестве объективного эмпирического фундамента для параметризации стохастических математических моделей.
Практическая ценность предложенной методики заключается в автоматизации формирования профилей уязвимости на современном уровне развития интеллектуальных технологий обработки больших массивов гетерогенных данных.
Перспективным направлением совершенствования представленного инструментария является разработка научно-методического аппарата оценки потенциальных (предельных) характеристик защищенности киберфизических объектов. В современной теории надежности программно-аппаратных комплексов активно развивается подход, при котором устойчивость рассматривается как непрерывный процесс функциональной деградации барьерных свойств системы $D(t)$. Аналогичный подход с учетом представленной выше методики целесообразно распространить на свойство кибернетической безопасности. Динамика информационного старения в таких моделях также будет описываться экспоненциальными законами, зависящими от интенсивности потока угроз λ.

Однако для того, чтобы математическая модель деградации адекватно отражала реальность, параметр интенсивности должен учитывать не только частоту публикации уязвимостей, но и их архитектурную тяжесть (разрушительный потенциал). Именно здесь результаты профилирования находят свое прямое применение.
Имея для выбранного стека технологий набор из N выделенных профилей уязвимостей (PF_j), каждый из которых обладает вычисленной статистической вероятностью p_j и нормализованным весом тяжести W_j, имеется возможность вычислить математическое ожидание ущерба от одной случайной угрозы:

$$\overline{W} = \sum_{j=1}^{N}(p_j \cdot W_j).$$

Подстановка эмпирически полученных значений p_j и W_j в данное уравнение решает главную проблему предиктивной безопасности – параметрическую неопределенность. Вместо использования субъективных экспертных оценок, системный архитектор оперирует объективными метриками, извлеченными из анализа сотен тысяч реальных исторических инцидентов.

Дальнейшее использование вычисленного математического ожидания $\overline{W}$ позволяет определить общую ожидаемую интенсивность деградации системы:

$$\lambda_{\text{exp}} = \nu \cdot \overline{\text{W}},$$

где ν – средняя частота выявления новых уязвимостей в анализируемом технологическом стеке за единицу времени.

Использование полученной интенсивности λ_{exp} в дифференциальных уравнениях надежности позволяет строить высокоточные графики прогнозируемого падения защищенности $D(t)$. Более того, применение аппарата дисперсии к базовым профилям дает возможность математически обосновать границы доверительных интервалов – оптимистичный и пессимистичный сценарии старения («воронку неопределенности»).
Таким образом, разработанная методика нормализации и кластеризации ретроспективных баз данных (*NVD*, БДУ ФСТЭК) предоставляет инженерам и аналитикам *SOC* достоверные количественные параметры. Эти параметры могут быть напрямую интегрированы в системы автоматизированного проектирования для расчета барьерных функций надежности, прогнозирования времени до критического отказа систем и риск-ориентированного планирования технологических окон для патч-менеджмента.
В представленной статье решена актуальная научно-практическая задача систематизации и интеллектуальной обработки ретроспективных массивов данных об угрозах информационной безопасности. Доказано, что глобальные базы уязвимостей (*NVD*, БДУ ФСТЭК России), несмотря на свою изначальную гетерогенность и неполноту, могут служить надежным эмпирическим фундаментом для параметризации предиктивных риск-моделей при условии применения соответствующих алгоритмов предварительной нормализации.
Разработанный комплексный подход профилирования позволяет осуществить качественный переход от хаотичного реактивного мониторинга единичных инцидентов к прогнозированию на макроуровне. Применение методов обработки естественного языка в синергии с плотностными алгоритмами машинного обучения обеспечило возможность трансформации сотен тысяч разрозненных текстовых отчетов и устаревших метрик в ограниченный набор формализованных математических сущностей - эталонных профилей уязвимостей.
Вычисление для каждого выделенного профиля статистической вероятности возникновения (p_j) и усредненного показателя тяжести (W_j) на базе современного стандартов *CVSS* решает фундаментальную проблему неопределенности в теории надежности программно-аппаратных систем.

ЗАКЛЮЧЕНИЕ

Таким образом, предложенная методика интеллектуального анализа данных формирует объективную количественную базу для построения стохастических моделей деградации барьерных функций. Внедрение разработанных алгоритмов профилирования открывает новые перспективы для автоматизации процессов безопасного проектирования в системах класса САПР, а также для перехода центров мониторинга на проактивное риск-ориентированное планирование патч-менеджмента и технического обслуживания критической инфраструктуры.

Направлениями дальнейших исследований целесообразно считать:

- разработку имитационной модели, базирующейся на выделенном множестве источников исходных данных и обеспечивающей проверку точности, чувствительности и устойчивости предложенного научно-методического инструментария;

- разработку алгоритмов прогнозирования профилей уязвимости и оптимизации характеристик защищенности критически важных киберфизических объектов для различных стеков применяемых технологий.

ЛИТЕРАТУРА

[1] Баранов А. П., Бочков М. В. Методика адаптивной оценки критичности уязвимостей в автоматизированных системах управления // Проблемы информационной безопасности. Компьютерные системы. – 2022. – № 3. – С. 15–23.

[2] Лукацкий А. В. Риск-ориентированное управление уязвимостями: от CVSS к реальным приоритетам // Вопросы защиты информации. – 2020. – № 4. – С. 12–18.

[3] Костров Д. В., Смирнов А. А. Оценка эффективности систем защиты информации в государственных информационных системах на основе риск-ориентированного подхода // Информация и безопасность. – 2023. – Т. 26, № 2. – С. 189–198.

[4] Гайдай, А.А. Непрерывный контроль процесса достижения цели / А.А. Гайдай, И.Б. Руссман // Управление большими системами: сб. трудов. – 2004. – № 7. – С. 106–113.

[5] Саитов И.А., Кунин Н.Т., Пиун П.В. Подход к оценке эффективности государственных информационных систем на базе развития метода траекторного анализа // IV ежегодная национальная научно-практическая конференция «Цифровизация правосудия: проблемы и перспективы». – 11-18 декабря 2025 г. – М., 2025. – 11 с.

[6] Гавдан Г. П. Управление безопасностью государственных информационных систем как объектов критической информационной инфраструктуры / Г. П. Гавдан, А. А. Голубев, А. Г. Голубев, И. Ю. Жуков, Э. П. Рыбалко // Безопасность информационных технологий (BIT) / Техническая безопасность. – 2025. – № 3. – С. 23–30.

[7] Шадский В. В., Сизоненко А. Б., Чекмарёв М. А., Шишков А. В., Исакин Д. А. Исследование способов векторизации неструктурируемых текстовых документов на естественном языке по степени их влияния на качество работы различных классификаторов // Научно-технический вестник информационных технологий, механики и оптики. – 2022. – Т. 22, № 1. – С. 114–119. – DOI: 10.17586/2226-1494-2022-22-1-114-119.

[8] Кравченко Ю. А., Мансур А. М. Векторизация текста с использованием методов интеллектуального анализа данных // Известия ЮФУ. Технические науки. – 2021.

[9] Kulkarni O. S. A Survey of Advancements in DBSCAN Clustering Algorithms for Big Data // 2024. – P. 106–111.

METHODOLOGY FOR DEVELOPING VULNERABILITY PROFILES OF PROTECTED OBJECTS BASED ON HISTORICAL DATA

I.A. Saitov, N.T. Kunin

Federal State Budgetary Educational Institution of Higher Education “MIREA – Russian Technological University”, Moscow, Russia, saitov_i@mirea.ru

Abstract: ensuring predictive cybersecurity for modern software and hardware protected objects requires a shift from qualitative threat assessments to rigorous quantitative models. A relevant scientific and technical challenge in parameterizing such models is determining the statistical probabilities and expected damage from future cyberattacks. This paper proposes a comprehensive methodology for developing “vulnerability profiles” based on the intelligent analysis of historical data from global and national databases. The main focus of the work is on methods for collecting, cleaning, and statistically clustering accumulated datasets of vulnerabilities. The study describes an algorithm for translating disparate metrics into standardized vectors, as well as the application of machine learning methods to group hundreds of thousands of incidents into a limited set of typified profiles. For each generated profile, the statistical probability of occurrence within a given technology stack and the expected severity weight of the consequences are calculated. The results of applying the proposed profiling tools provide researchers and system architects with reliable empirical data that can be directly used as input parameters for stochastic risk models, calculation of reliability barrier functions, and automation of predictive patch management.

Keywords: predictive security, vulnerability profile, retrospective analysis, data mining, threat clustering, vulnerability databases, statistical probability assessment.