БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 4 (115). – 9–24

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.5 DOI: 10.17212/2782-2230-2024-4-9-24

МОДЕЛЬ МАШИННОГО ОБУЧЕНИЯ ПРИ АНАЛИЗЕ УГРОЗ В КОМПОЗИТНОЙ АРХИТЕКТУРЕ БЕЗОПАСНОСТИ*

А.В. ПИЛЕЦКАЯ[1], С.П. ОРЛОВ[2]

[1] *443100, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, аспирант кафедры информатики и вычислительной техники. E-mail: piletskaya.tonya@gmail.com*
[2] *443100, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, профессор кафедры информатики и вычислительной техники. E-mail: orlovsp1946@gmail.com*

В настоящее время возрастает число кибератак на различные информационные системы. В связи с этим перспективным является построение композитной архитектуры безопасности. Композитная архитектура безопасности объединяет различные методы и модели в единую систему. Модульность и гибкость такой архитектуры особенно эффективна при защите распределенных информационных систем. При этом важной задачей является исследование потенциального влияния различных угроз на целостность данных, уровень защищенности, обеспечение безопасного межсетевого взаимодействия. В статье выполнен анализ различных моделей угроз. Предложено применение машинного обучения на основе алгоритма Isolation Forest. Для иллюстрации при анализе угроз выбрана модель STRIDE. Разработана программа на языке Python для реализации метода изолирующего леса Isolation Forest с целью выявления аномалий в трафике данных. Приведены результаты в виде графиков основных параметров: количество запросов, объем данных и время отклика. С помощью модели Silhouette Score выполнена оценка качества обучения. Внедрение машинного обучения в комбинации с различными методами защиты поможет решить проблему безопасности архитектуры приложения и построить взаимозаменяемую модульную структуру.

Ключевые слова: защита информации, архитектура безопасности, модели угроз, аномалии сетевого трафика, машинное обучение

* Статья получена 10 ноября 2024 г.

ВВЕДЕНИЕ

Современные информационные системы сталкиваются с постоянно возрастающей угрозой кибератак, что требует разработки более продвинутых и гибких мер безопасности. Хотя традиционные способы защиты, такие как межсетевые экраны, системы обнаружения вторжений и шифрование, остаются важными, они уже не способны полностью справляться с быстро изменяющимися атаками, которые используют новые уязвимости. Исследования показали, что в 2022 году зарубежные предприятия в среднем использовали более 130 инструментов безопасности. При этом такие инструменты создают дополнительные проблемы в управлении, требуют большего количества рабочей силы и занимают значительную часть бюджета безопасности [1]. В этих условиях внедрение машинного обучения (ML) при создании композитной архитектуры безопасности открывает новые возможности для динамической защиты и оперативного анализа угроз.

Композитная архитектура безопасности – это методика построения системы, использующая различные технологии и методы для создания многослойной и интегрированной системы защиты [2, 3]. Один из примеров такого подхода – архитектура Cybersecurity Mesh Architecture (CSMA), предложенная в [4]. Эта архитектура фокусируется на модульности и гибкости в защите распределенных активов и ресурсов организации. Она поддерживает координацию между различными продуктами безопасности, создавая более целостную и адаптивную среду безопасности, вместо того чтобы полагаться на разрозненные решения. В условиях цифровой трансформации и гибридных рабочих процессов эта архитектура позволяет повысить защиту за счет интеграции и масштабируемости.

Композитная архитектура безопасности базируется на идее интеграции различных технологий, методов и стратегий защиты в единую систему. Этот подход позволяет обеспечить более высокий уровень безопасности, что особенно важно для сложных и распределенных инфраструктур, таких как облачные решения, интернет вещей (IoT) и микросервисные приложения. Машинное обучение в такой архитектуре помогает автоматизировать анализ данных и адаптировать защитные меры на основе поведения системы, анализа сетевого трафика и активности пользователей. Внедрение машинного обучения в комбинации с различными методами защиты поможет решить проблему сочетания различных подходов к безопасности приложений и выстроить взаимозаменяемую модульную архитектуру безопасности.

Целью исследования настоящей работы является анализ применения машинного обучения для создания композитной архитектуры безопасности, способной выявлять уже известные угрозы и адаптироваться к появлению

новых видов атак. Основное внимание уделяется тому, каким образом модели машинного обучения могут быть встроены на различные уровни системы безопасности, начиная с сетевых протоколов и заканчивая приложениями и системами хранения данных.

1. АКТУАЛЬНОСТЬ ПРОБЛЕМЫ

С развитием информационных технологий и цифровизации бизнеса организации сталкиваются с растущими рисками в киберпространстве. По данным Global Risk Report Всемирного экономического форума, кибератаки и утечки данных остаются наиболее значимыми угрозами для организаций всех масштабов [4]. Традиционные подходы к защите, такие как брандмауэры и антивирусные программы, уже не могут справляться с современными угрозами, так как атаки становятся более сложными, распределенными и автоматизированными.

Особую опасность представляют собой целевые атаки (targeted attacks), которые используют слабые места в архитектуре систем для проникновения внутрь сети. Примерами таких атак является использование уязвимостей в межкомпонентных взаимодействиях микросервисов или несанкционированный доступ к облачным ресурсам. В этих условиях необходимость интеграции адаптивных мер безопасности становится ключевой задачей для повышения устойчивости систем к атакам.

Построение композитной архитектуры безопасности системы включает следующие этапы:

1) анализ современных угроз для распределенных систем и разработка композитных решений безопасности;

2) внедрение адаптивных методов защиты, которые могут динамически изменять конфигурацию системы в зависимости от типа угрозы;

3) применение методов машинного обучения для автоматического выявления аномалий и реагирования на киберугрозы.

2. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

2.1. АНАЛИЗ СУЩЕСТВУЮЩИХ МОДЕЛЕЙ УГРОЗ

В настоящее время известно много методов и технологий защиты при проектировании архитектуры информационной системы. Большое внимание уделяется разработке и исследованию моделей угроз в различных информа-

ционных системах [5, 6]. Рассмотрим ряд методов и моделей, которые могут быть положены в основу при использовании машинного обучения для защиты компонентов системы и выявления потенциальных угроз. В таблице представлены модели угроз с разными подходами по их выявлению.

Основные методы и модели угроз

Basic threat techniques and models

Методика	Описание	Цель	Применение
STRIDE [7]	Модель угроз, разработанная Microsoft и направленная на выявление шести основных типов угроз	Идентификация и классификация угроз	Используется для анализа безопасности приложений и систем
PASTA [8]	Анализ угроз, ориентированный на атаку, включает семь этапов оценки рисков для бизнеса	Анализ рисков безопасности	Применяется для анализа атак и их влияния на бизнес
LIDDUN [9]	Моделирование угроз для защиты конфиденциальности (privacy threats)	Защита конфиденциальности	Уделяется внимание вопросам конфиденциальности данных
Attack Trees [10]	Представляет угрозы как дерево решений, где каждый узел – это цель, а ветви – возможные пути атаки	Визуализация и анализ возможных атак	Используется для структурирования атак и анализа путей проникновения
OCTAVE [11]	Методика управления рисками, разработанная для анализа и управления киберрисками	Анализ и управление рисками безопасности	Подходит для организационного анализа безопасности

Окончание таблицы

Методика	Описание	Цель	Применение
NIST [12]	Стандартный фреймворк для управления кибербезопасностью. Основан на рекомендациях NIST	Управление киберрисками	Универсальный инструмент для организаций любого масштаба
TRIKE [13]	Методика моделирования угроз, основанная на оценке рисков и ролей пользователей	Оценка и моделирование угроз	Применяется для безопасности систем с ролевой моделью
Kill Chain [14]	Модель атак на основе анализов этапов атаки (например, разведка, доставка, эксплуатация)	Анализ последовательности кибератак	Используется для анализа и предотвращения целенаправленных атак
VAST [15]	Комплексная методология безопасности	Создание визуальных моделей угроз. Архитектурные угрозы отображаются с помощью диаграмм потоков процессов, а операционные угрозы детализируются с помощью диаграмм потоков данных	Модель разработана для использования в Agile- и DevOps-процессах. Этот подход помогает вовлечь всю команду разработки и безопасности в процесс управления рисками и ускорить выявление уязвимостей на ранних этапах

Далее в статье рассматривается модель STRIDE для обоснования применения машинного обучения. Это обосновано тем, что эта модель включает шесть основных типов угроз, достаточно простая и эффективно применяется в программных приложениях.

2.2. ПРИМЕНЕНИЕ МЕТОДА МАШИННОГО ОБУЧЕНИЯ

При проектировании композитной архитектуры безопасности машинное обучение позволяет анализировать большие объемы данных, автоматически выявлять аномалии, предсказывать потенциальные атаки и предлагать соответствующие меры защиты [16]. Применение машинного обучения открывает следующие возможности:

- для выявления подозрительных действий, которые отклоняются от нормального поведения;
- обучения на реальных данных для определения паттернов, которые указывают на возможные атаки;
- создания систем с автоматическим реагированием на инциденты.

В качестве примера рассматривается разработанная программа, часть кода которой на языке Python приведена ниже.

В алгоритме была использована модель машинного обучения Isolation Forest [17] для обнаружения аномалий (или выбросов) в данных.

Основная идея алгоритма:

- изоляция аномалий путем построения деревьев решений, которые разрезают данные на части. Аномалии проще «изолировать», так как они более удалены от нормальных точек;
- это метод без учителя. Это означает, что он не требует проставления меток для аномальных событий и работает на основе структуры исходных данных.

Алгоритм реализуется в виде следующих этапов.

1. Генерация данных. Код создает два набора данных: нормальный сетевой трафик и аномальный. Это упрощенный пример, где количество запросов, объем данных и время отклика используются как признаки.

2. Предварительная обработка данных. Данные стандартизируются с использованием StandardScaler, чтобы все признаки имели одинаковую шкалу, что улучшает работу алгоритма.

3. Обучение модели. Используется модель Isolation Forest, которая обучается на данных и автоматически определяет, какие из них являются аномальными. Алгоритм работает, изолируя аномальные точки данных с помощью деревьев решений

4. Предсказание аномалий. После обучения модель классифицирует каждую запись как нормальную или аномальную.

5. Визуализация. В результате выводятся графики (рис. 1–4) с нормальным трафиком и аномальными точками.

Фрагменты кода программы для анализа угроз типа STRIDE приведены на листинге 1 и листинге 2.

Листинг 1 – Код программы

```
    # Импорт библиотек
    import numpy as np
    import pandas as pd
    from sklearn.ensemble import IsolationForest
    from sklearn.preprocessing import StandardScaler
    import matplotlib.pyplot as plt
    from matplotlib.dates import DateFormatter

    # STRIDE Угрозы
    stride_threats = {
        "Spoofing": "Подделка запросов или идентификаторов
пользователей",
        "Tampering": "Модификация данных",
        "Repudiation": "Отказ от действий",
        "Information Disclosure": "Разглашение информации",
        "Denial of Service": "Отказ в обслуживании",
        "Elevation of Privilege": "Повышение привилегий"
    }
    # Функция для генерации синтетических данных с имитацией
угроз STRIDE
    def generate_synthetic_traffic_with_threats():
        np.random.seed(42)
        # Обычный трафик
        normal_traffic = np.random.normal(loc=10, scale=2,
size=(1000, 3))

        # Создание аномального трафика с имитацией угроз
STRIDE
        threats_traffic = {
            "Spoofing": np.random.normal(loc=20, scale=5,
size=(20, 3)),  # Подделка
            "Tampering": np.random.normal(loc=30, scale=6,
size=(20, 3)),  # Модификация данных
            "Denial of Service": np.random.normal(loc=50,
scale=7, size=(20, 3)),  # DDoS-атаки
            "Information Disclosure":
np.random.normal(loc=40, scale=4, size=(20, 3)),  # Утечка
данных
        }
```

Листинг 2 – Продолжение кода программы

```
    # Объединение обычного и аномального трафика
        data = np.vstack((normal_traffic,
*threats_traffic.values()))
        df = pd.DataFrame(data, columns=["num_requests", "da-
ta_volume_mb", "response_time_ms"])
        df["timestamp"] = timestamps

      return df

    # Генерация трафика с угрозами
    df = generate_synthetic_traffic_with_threats()

    # Стандартизация данных
    scaler = StandardScaler()
    df_scaled = scaler.fit_transform(df[["num_requests", "da-
ta_volume_mb", "response_time_ms"]])

    # Обучение Isolation Forest для выявления аномалий
    iso_forest = IsolationForest(contamination=0.1, ran-
dom_state=42)
    df["is_anomaly"] = iso_forest.fit_predict(df_scaled)
    df["is_anomaly"] = df["is_anomaly"].apply(lambda x: "Anoma-
ly" if x == -1 else "Normal")

    # Отображение аномалий и тип угрозы
    print(f"Количество обнаруженных аномалий:
{df['is_anomaly'].value_counts()['Anomaly']}")

    # Визуализация временных рядов с угрозами
    def plot_stride_threats(df):
        fig, ax = plt.subplots(figsize=(12, 6))

        normal_data = df[df["is_anomaly"] == "Normal"]
        anomalous_data = df[df["is_anomaly"] == "Anomaly"]

plot_stride_analysis(df)
```

Данные, которые использует приложение, являются синтетическими. Функция generate_synthetic_traffic() с помощью библиотеки NumPy создает два набора данных:

- Нормальный трафик (normal_traffic): модель генерирует 1000 записей с нормальным законом распределением трафика, где каждое значение имеет среднее, равное 10, и стандартное отклонение, равное 2.
- Аномальный трафик (anomalous traffic).

На рис. 1 показаны различные виды угроз STRIDE:

- Spoofing (подделка запросов);
- Tampering (модификация данных);
- Denial of Service (отказ в обслуживании);
- Information Disclosure (разглашение информации).

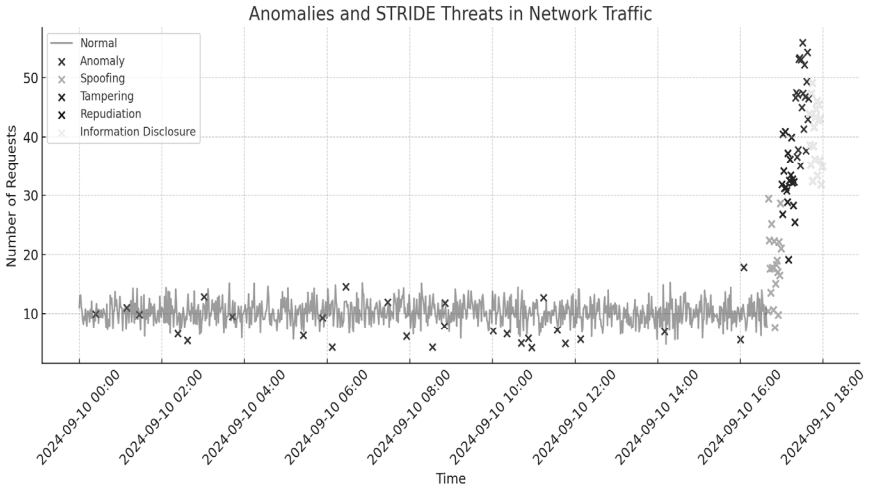

Рис. 1. Временной ряд с аномалиями и угрозами STRIDE

Fig. 1. The time series with anomalies and threats STRIDE

На следующих графиках (рис. 2–4) показана связь угроз STRIDE с тремя ключевыми метриками: количество запросов, объем данных и время отклика. На этих рисунках горизонтальная ось Index обозначает индексы строк в DataFrame. Они напрямую связаны не с временными метками, а, скорее, с порядковыми номерами данных после их создания. Визуализация использует индексы, чтобы показать, как изменяются значения (например, количество

запросов, объем данных и время отклика) по мере поступления новых данных. Если необходимо привязать график к временным меткам, то можно использовать столбец timestamp в качестве значений для горизонтальной оси графиков.

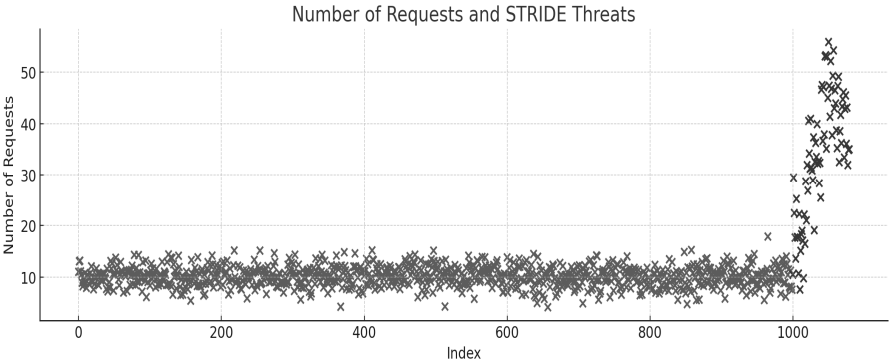

Рис. 2. Общее количество запросов и число запросов с угрозами STRIDE

Fig. 2. The total number of requests and number of requests with STRIDE threats

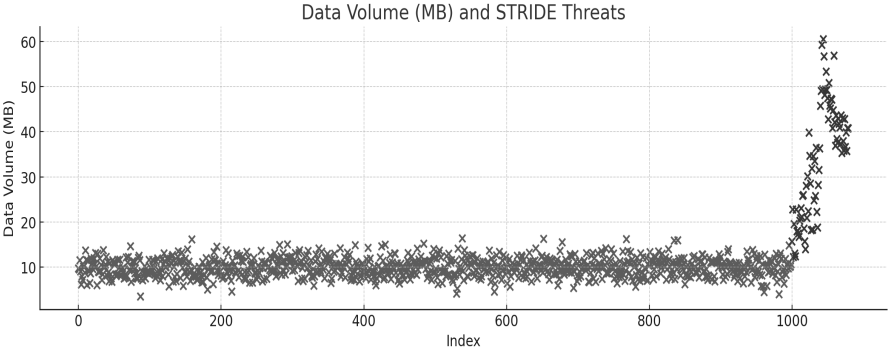

Рис. 3. Объем данных с угрозами STRIDE, Мбайт

Fig. 3. Data Volume with STRIDE threats, MB

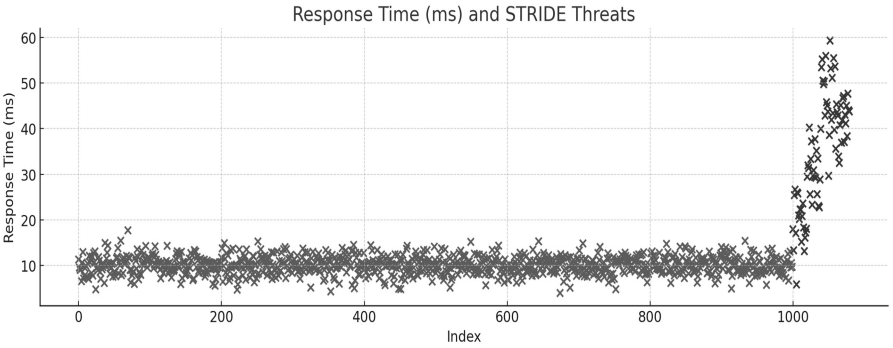

Рис. 4. Время отклика при наличии угроз STRIDE, мс

Fig. 4. The response time in the presence of STRIDE threats, ms

Анализ этих графиков позволяет понять, как разные угрозы STRIDE влияют на поведение системы.

Например:

а) атаки типа Tampering могут существенно влиять на количество запросов, но не увеличивать значительно объем данных;

б) атаки типа Denial of Service могут увеличить время отклика до неприемлемо больших значений.

Оценка качества обучения проводилась с использованием модели Silhouette Score. Модель разделяет данные на нормальные события и аномальные явления и может использоваться в задачах кластеризации. Полученное значение silhouette_score = 0.7770604900198429 указывает на то, что разделение между нормальными и аномальными точками относительно сильное: значения, близкие к единице, указывают на более четко выраженные кластеры.

ЗАКЛЮЧЕНИЕ

Композитная архитектура безопасности представляет собой эволюцию традиционных методов защиты в условиях современных угроз. За счет интеграции адаптивных механизмов на основе поведенческого анализа и машинного обучения такие системы могут не только реагировать на уже известные угрозы, но и адаптироваться к новым, более сложным атакам. Рассмотренный в работе пример подтверждает вывод о перспективности использования методов машинного обучения при анализе угроз. В дальнейшем исследование композитной архитектуры с помощью методов машинного обучения позволит

улучшить защиту современных информационных систем и обеспечить их устойчивость к постоянно меняющимся вызовам в киберпространстве.

СПИСОК ЛИТЕРАТУРЫ

1. *Ariganello J.* More is Less: the challenge of utilizing multiple security tools // Anomali. Blog: website. – 2022. – April 13. – URL: https://www.anomali.com/blog/more-is-less-the-challenge-of-utilizing-multiple-security-tools (accessed: 29.11.2024).

2. *Куликовский Д.О., Халина Д.Н.* Анализ процесса создания безопасной информационной системы предприятия // Безопасность цифровых технологий. – 2023. – № 4 (111). – С. 35–46. – DOI: 10.17212/2782-2230-2023-4-35-46.

3. *Sathiaseelan J.G.R.* Architectural framework for secure composite web services // International Journal of Computer Applications. – 2013. – Vol. 76 (1). – P. 18–23. – DOI: 10.5120/13211-0592.

4. *Arora S.* From chaos to confidence: the indispensable role of security architecture // ISAKA: website. – 2023. – 7 November. – URL: https://www.isaca.org/resources/news-and-trends/industry-news/2023/from-chaos-to-confidence-the-indispensable-role-of-security-architecture (accessed: 29.11.2024).

5. *Дураковский А.П., Цимбал В.Н.* Моделирование угроз безопасности информации беспроводного стандарта IEEE 802.11 // Безопасность информационных технологий. – 2022. – Т. 29, № 4. – С. 42–52. – DOI: 10.26583/bit.2022.4.04.

6. *Гарбук С.* Функциональность и безопасность систем искусственного интеллекта: качество данных // Открытые системы. СУБД. – 2024. – № 1. – С. 18–22. – DOI: 10.51793/OS.2024.95.90.004.

7. Microsoft Learn. The STRIDE threat model. AI skills challenge. 2009. – URL: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN (accessed: 29.11.2024).

8. *Allen-Addy C.* Threat modeling methodology: PASTA // IriusRisk: website. – 2023. – September 29. – URL: https://www.iriusrisk.com/resources-blog/pasta-threat-modeling-methodologies (accessed: 29.11.2024).

9. LINDDUN methods // LINDDUN: website. – URL: https://linddun.org/methods/ (accessed: 29.11.2024).

10. *Schneier B.* Attack Trees // Schneier on Security. Blog: website. – 1999. – URL: https://www.schneier.com/academic/archives/1999/12/attack_trees.html (accessed: 29.11.2024).

11. OCTAVE Method Implementation Guide. Version 2.0. Vol. 1: Introduction / Software Engineering Institute. – URL: https://insights.sei.cmu.edu/library/

octave-method-implementation-guide-version-20-volume-1-introduction/ (accessed: 29.11.2024).

12. NIST Releases Version 2.0 of Landmark Cybersecurity Framework // NIST: website. – 2024. – February 26. – URL: https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework (accessed: 29.11.2024).

13. *Eddington M., Larcom B., Saitta E.* Trike v1 Methodology Document [Draft], 2005. – URL: https://trike.sourceforge.net/papers/ (accessed: 29.11.2024).

14. Lockheed Martin. The Cyber Kill Chain. – URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html/ (accessed: 29.11.2024).

15. VAST. Security. Protecting Data is a Business and Ethical Imperative. – URL: https://vastitservices.com/it-strategy/security/ (accessed: 29.11.2024).

16. *Исхаков А.Ю., Гайдук К.А.* Проактивный поиск внутренних угроз информационной безопасности в условиях ограничений // Вопросы кибербезопасности. – 2023. – № 4 (56). – С. 105–119. – DOI: 10.21681/2311-3456-2023-4-105-119.

17. *Liu F.T., Ting K.M., Zhou Z.-H.* Isolation-based anomaly detection // ACM Transactions on Knowledge Discovery from Data (TKDD). – 2012. – Vol. 6 (1). – P. 1–39. – DOI: 10.1145/2133360.2133363.

Пилецкая Антонина Валерьевна, аспирант кафедры информатики и вычислительной техники Самарского государственного технического университета. Основное направление научных исследований – информационная безопасность систем обработки данных. E-mail: piletskaya.tonya@gmail.com

Орлов Сергей Павлович, доктор технических наук, профессор кафедры информатики и вычислительной техники Самарского государственного технического университета. Область научных интересов – системы искусственного интеллекта, математическое моделирование сложных систем. E-mail: orlovsp1946@gmail.com

DOI: 10.17212/2782-2230-2024-4-9-24

Machine learning model for threat analysis in composite security architecture *

A.V. Piletskaya[1], S.P. Orlov[2]

[1] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, postgraduate of the Informatics and Computer Technology Department. E-mail: piletskaya.tonya@gmail.com*
[2] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, doctor of technical science, professor of the Informatics and Computer Technology Department. E-mail: orlovsp1946@gmail.com*

Currently, the number of cyber-attacks on various information systems is increasing. In this regard, the construction of composite security architecture is promising. Composite security architecture combines various methods and models into a single system. The modularity and flexibility of such architecture is especially effective in protecting distributed information systems. An important task is to study the potential impact of various threats on data integrity, the level of security, and ensuring secure inter-network interaction. The article analyzes various threat models. The application of machine learning based on the Isolation Forest algorithm is proposed. The STRIDE model is selected to illustrate the analysis of threats. A Python program has been developed to implement the Isolation Forest method to identify anomalies in data traffic. The results are presented in the form of graphs of the main parameters: number of requests, data volume, and response time. Silhouette Score model was used to assess the quality of training. The implementation of machine learning in combination with various security methods will help solve the problem of application architecture security and build an interchangeable modular structure.

Keywords: information security, security architecture, threat models, network traffic anomalies, machine learning

REFERENCES

1. Ariganello J. More is Less: the challenge of utilizing multiple security tools. *Anomali. Blog*. Website, 2022, April 13. Available at: https://www.anomali.com/blog/more-is-less-the-challenge-of-utilizing-multiple-security-tools (accessed 29.11.2024).

2. Kulikovskij D.O., Khalina D.N. Analiz protsessa sozdaniya bezopasnoi informatsionnoi sistemy predpriyatiya [Analysis creation process of a secure enterprise information system]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 4 (111), pp. 35–46. DOI: 10.17212/2782-2230-2023-4-35-46.

* *Received 10 November 2024.*

3. Sathiaseelan J.G.R. Architectural framework for secure composite web services. *International Journal of Computer Applications*, 2013, vol. 76 (1), pp. 18–23. DOI: 10.5120/13211-0592.

4. Arora S. From chaos to confidence: the indispensable role of security architecture. *ISAKA*. Website, 2023, 7 November. Available at: https://www.isaca.org/resources/news-and-trends/industry-news/2023/from-chaos-to-confidence-the-indispensable-role-of-security-architecture (accessed 29.11.2024).

5. Durakovskiy A.P., Tsimbal V.N. Modelirovanie ugroz bezopasnosti informatsii besprovodnogo standarta IEEE 802.11 [Modelling of information security threats for the wireless standard IEEE 802.11]. *Bezopasnost' informatsionnykh tekhnologii = IT Security (Russia)*, 2022, vol. 29, no. 4, pp. 42–52. DOI: 10.26583/bit.2022.4.04.

6. Garbuk S. Funktsional'nost' i bezopasnost' sistem iskusstvennogo intellekta: kachestvo dannykh [Functionality and security of artificial intelligence systems: data quality]. *Otkrytye sistemy. SUBD = Open Systems. DBMS*, 2024, no. 1, pp. 18–22. DOI: 10.51793/OS.2024.95.90.004.

7. Microsoft Learn. *The STRIDE threat model. AI skills challenge*. 2009. Available at: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN (accessed 29.11.2024).

8. Allen-Addy C. Threat modeling methodology: PASTA. *IriusRisk*. Website, 2023, September 29. Available at: https://www.iriusrisk.com/resources-blog/pasta-threat-modeling-methodologies (accessed 29.11.2024).

9. LINDDUN methods. *LINDDUN*. Website. Available at: https://linddun.org/methods/ (accessed 29.11.2024).

10. Schneier B. Attack Trees. *Schneier on Security. Blog*. Website, 1999. Available at: https://www.schneier.com/academic/archives/1999/12/attack_trees.html (accessed 29.11.2024).

11. Software Engineering Institute. *OCTAVE Method Implementation* Guide. Version 2.0. Vol. 1: *Introduction.* Available at: https://insights.sei.cmu.edu/library/octave-method-implementation-guide-version-20-volume-1-introduction/ (accessed 29.11.2024).

12. NIST Releases Version 2.0 of Landmark Cybersecurity Framework. *NIST*. Website, 2024, February 26. Available at: https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework (accessed 29.11.2024).

13. Eddington M., Larcom B., Saitta E. *Trike v1 Methodology Document [Draft]*, 2005. Available at: https://trike.sourceforge.net/papers/ (accessed 29.11.2024).

14. Lockheed Martin. *The Cyber Kill Chain*. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html/ (accessed 29.11.2024).

15. VAST. *Security. Protecting Data is a Business and Ethical Imperative*. Available at: https://vastitservices.com/it-strategy/security/ (accessed 29.11.2024).

16. Iskhakov A. IU., Gaiduk K. A. Proaktivnyi poisk vnutrennikh ugroz informatsionnoi bezopasnosti v usloviiakh ogranichenii [Proactive search for internal threats to information security in conditions of constraints]. *Voprosy kiberbezopasnosti = Cybersecurity Issues*, 2023, no. 4 (56), pp. 105–119. DOI: 10.21681/2311-3456-2023-4-105-119.

17. Liu F.T., Ting K.M., Zhou Z.-H. Isolation-based anomaly detection. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 2012, vol. 6 (1), pp. 1–39. DOI: 10.1145/2133360.2133363.

Для цитирования:

Пилецкая А.В., Орлов С.П. Модель машинного обучения при анализе угроз в композитной архитектуре безопасности // Безопасность цифровых технологий. – 2024. – № 4 (115). – С. 9–24. – DOI: 10.17212/2782-2230-2024-4-9-24.

For citation:

Piletskaya A.V., Orlov S.P. Model' mashinnogo obucheniya pri analize ugroz v kompozitnoi arkhitekture bezopasnosti [Machine learning model for threat analysis in composite security architecture]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 4 (115), pp. 9–24. DOI: 10.17212/2782-2230-2024-4-9-24.