Математические структуры и моделирование
2024. № 4 (72). С. 111–124

УДК 004.056.53
DOI 10.24147/2222-8772.2024.4.111-124

ВОЗМОЖНОСТИ ИИ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ: ВОПРОСЫ ОБНАРУЖЕНИЯ, ПРЕДОТВРАЩЕНИЯ И РЕАГИРОВАНИЯ НА SQL-ИНЪЕКЦИИ, XSS- И CSRF-АТАКИ

Д.Э. Вильховский
старший преподаватель, e-mail: vilkhovskiy@gmail.com

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Представлен обзор возможностей применения искусственного интеллекта для усиления кибербезопасности веб-приложений с акцентом на обнаружение, предотвращение и реагирование на SQL-инъекции, XSS- и CSRF-атаки. Обсуждаются методы машинного обучения, такие как SVM, наивный байесовский алгоритм, ансамблевое и глубокое обучение, а также их интеграция с существующими системами безопасности. Включены гибридные модели и подходы к адаптации систем к новым угрозам. Также анализируются существующие проблемы и определены направления будущих исследований для преодоления этих вызовов.

Ключевые слова: компьютерная безопасность, информационная безопасность, кибербезопасность, SQL-инъекции, XSS-атаки, CSRF-атаки, машинное обучение, искусственный интеллект.

Введение

В современном мире киберугрозы становятся всё более сложными и разнообразными, что требует от организаций постоянного совершенствования своих стратегий информационной безопасности. Согласно отчёту по кибербезопасности [1], в 2023 г. наблюдался значительный рост кибератак. В частности, такие атаки, как SQL-инъекции, XSS и CSRF, остаются одними из наиболее распространённых и опасных. Например, согласно этому отчёту, в 2023 г. было зафиксировано более крупных 2,700 организаций, пострадавших от уязвимости SQL-инъекций. Эти атаки могут привести к утечке конфиденциальной информации и нарушению работы систем, что делает их приоритетной целью для предотвращения и реагирования.

Одной из ключевых технологий, способных значительно повысить уровень защиты, является искусственный интеллект (ИИ). Используя сложные алгоритмы, ИИ может быстро выявлять подозрительные паттерны и аномалии, что позволяет предотвращать атаки на ранних стадиях. Это особенно важно в условиях, когда атаки становятся всё более изощрёнными и частыми. Кроме того, ИИ может значительно сократить время и ресурсы, необходимые для реагирования на инциденты.

Таким образом, интеграция ИИ в системы кибербезопасности, особенно в области обнаружения, предотвращения и реагирования на SQL-инъекции, XSS и

CSRF-атаки, является актуальной и необходимой мерой для защиты организаций от современных киберугроз.

1. Возможности ИИ в обнаружении, предотвращении и реагировании на SQL-инъекции

Атаки с использованием SQL-инъекций остаются значительной угрозой для веб-приложений, используя уязвимости для получения несанкционированного доступа к базам данных, а также позволяя злоумышленникам выполнять несанкционированные SQL-команды. Поэтому необходимо разрабатывать решения, позволяющие повысить надёжность защиты организаций от SQL-инъекций, одним из которых является использование ИИ.

Проведём краткий обзор возможностей ИИ в обнаружении, предотвращении и реагировании на SQL-инъекции.

1.1. Возможности использования ИИ в области обнаружения SQL-инъекций

Использование ИИ повышает эффективность обнаружения атак с использованием SQL-инъекций.

1. **Метод опорных векторов и наивный байесовский алгоритм.** Данные алгоритмы могут эффективно использоваться для обнаружения и классификации атак с использованием SQL-инъекций. Исследование [2] показало, что использование метода опорных векторов (SVM) позволяет определить SQL-инъекции в 99,08 %. В работе [3] наивный байесовский алгоритм также характеризуется как наиболее эффективная модель с показателем обнаружения 97,06 %. Наконец, согласно исследованиям [4] и [5], интерпретируемость моделей SVM и наивного байесовского алгоритма также находится на высоком уровне, что подчёркивает необходимость их использования в процессах принятия решений при классификации SQL-команд. Указывается, что, постоянно обновляя данные для обучения, эти модели могут быстро адаптироваться к новым шаблонам атак.

2. **Ансамблевое обучение.** Такие методы, как Random Forest и AdaBoost, показали себя многообещающими в обнаружении SQL-инъекций. В работах [6] и [3] подчёркивается эффективность использования ансамблевых методов, таких как Gradient Boosting Machine (GBM) и Light Gradient Boosting Machine (LGBM), достигающих высокой точности и низкого уровня ложных срабатываний. В исследовании [7] предлагается архитектура глубокого обучения с использованием автокодировщиков RNN, точность которой достигает 94 %.

3. **Модели глубокого обучения.** Свёрточные нейронные сети (CNN) и сети с долговременной краткосрочной памятью (LSTM) использовались для обнаружения атак SQL-инъекций. Подход на основе CNN, разработанный и описанный в работе [8], продемонстрировал более высокую точность и устойчивость

к запутыванию по сравнению с традиционными методами. Исследование [9] также показывает высокую точность этих моделей в захвате синтаксиса и семантических особенностей SQL-запросов. В целом использование глубокого обучения повышает способность системы обобщать данные обучения, повышая точность обнаружения.

4. **Гибридные модели.** Гибридная модель CNN-BiLSTM, предложенная в работе [10], также позволяет достигнуть высокой точности в обнаружении атак SQL-инъекций, используя для повышения эффективности обнаружения сильные стороны свёрточных нейронных сетей и сетей с долговременной краткосрочной памятью.

5. **Извлечение признаков и векторизация.** В исследованиях [11, 12] рассматриваются вопросы интеграции этих методов с моделями машинного обучения, позволяющими повысить точность обнаружения SQL-инъекций посредством предварительной обработки SQL-запросов для лучшей методы классификации.

6. **Семантическое обучение.** Так, в работе [13] для улучшения обнаружения SQL-инъекций путём внедрения семантической информации на уровне предложений из SQL-операторов предлагается использование моделей семантического обучения, таких как synBERT.

7. **Генеративно-состязательные сети (GAN).** В работе [13] описывается использование GAN для генерации образцов SQL-инъекций. Отмечается, что это позволяет улучшить обучающие наборы данных для моделей обнаружения.

8. **Адаптивный глубокий лес (Adaptive Deep Forest).** В исследовании [14] предлагается использование метода Адаптивного глубокого леса. Доказывается, что данный метод позволяет оптимизировать структуру в соответствующих алгоритмах для обработки сложных атак SQL-инъекций, демонстрируя лучшую производительность, чем классические методы машинного обучения.

1.2. Возможности использования ИИ в области предотвращения атак с использованием SQL-инъекций

Интегрируя ИИ в стратегии предотвращения SQL-инъекций, организации могут значительно повысить уровень своей безопасности.

1. **Брандмауэры веб-приложений с встроенными ИИ-инструментами.** Интеграция ИИ в сетевые экраны повышает их способность обнаруживать и блокировать вредоносные SQL-запросы. Например, в работе [15] рассматривается, как фреймворк с использованием ИИ позволяет выявлять и смягчать попытки SQL-инъекции, даже когда злоумышленники используют методы мутации.

2. **Методы глубокого обучения.** В исследовании [9] доказывается, что посредством изучения сложных шаблонов в SQL-запросах CNN и рекуррентные нейронные сети (RNN) способны предотвращать даже сложные атаки.

3. **Гибридные модели.** Объединение различных методов ИИ может улучшить возможности предотвращения. Например, в работе [16] отмечается, что гибридный подход, использующий как статический, так и динамический анализ, может эффективно предотвращать атаки SQL-инъекций, анализируя структуры запросов и поведение во время выполнения.

4. **Применении ИИ для безопасного кодирования.** В исследованиях [17, 18] рассматриваются возможности ИИ в обеспечении соблюдения методов безопасного кодирования, таких как использование параметризованных запросов и проверка ввода пользователя. Также инструменты на основе ИИ могут автоматически анализировать код на наличие уязвимостей, предлагая улучшения для предотвращения атак с использованием SQL-инъекций, что помогает разработчикам выявлять и устранять потенциальные проблемы безопасности до того, как они будут использованы.

1.3. Возможности использования ИИ в области реагирования на атаки с использованием SQL-инъекций

Механизмы реагирования на атаки с использованием SQL-инъекций имеют решающее значение для смягчения воздействия этих угроз после их обнаружения. Решения на основе ИИ предлагают расширенные возможности для реагирования и смягчения в реальном времени, повышая безопасность веб-приложений.

1. **Автоматизированные системы реагирования с использованием моделей машинного обучения.** В работах [19, 20] указывается, что использование моделей машинного обучения, таких как основанные на архитектурах глубокого обучения, позволяет не только быстро идентифицировать вредоносные запросы, но и немедленно применять контрмеры. Например, эти системы могут выполнять предопределённые протоколы реагирования, такие как изоляция затронутых систем или откат вредоносных транзакций, чтобы минимизировать ущерб [21].

2. **Динамическая очистка запросов с использованием ИИ.** В исследовании [22] рассматриваются вопросы динамической очистки SQL-запросы инструментами, использующими алгоритмы ИИ, и отмечается, что использование ИИ действительно позволяет быстро предотвратить выполнение вредоносного кода.

3. **Интеграция с системами обнаружения вторжений (IDS).** IDS-системы с использованием ИИ-инструментов позволяют улучшить их возможности обнаружения и реагирования. Так, используя алгоритмы машинного обучения, эти системы могут лучше определять аномальное поведение, указывающее на попытки SQL-инъекций, и инициировать соответствующие ответы [23].

2. Возможности ИИ в обнаружении, предотвращении и реагировании на XSS-атаки

Атаки с подделкой межсайтовых запросов (Cross-Site Request Forgery, CSRF-атаки) представляют собой серьёзную угрозу для веб-приложений, позволяя злоумышленникам выполнять несанкционированные действия от имени пользователей. Применение ИИ в этой области позволяет автоматизировать процесс обнаружения и реагирования на такие угрозы.

2.1. Возможности использования ИИ в области обнаружения XSS-атак

ИИ предоставляет значительные возможности для обнаружения XSS-атак.

1. **SVM и наивный байесовский алгоритм.** Исследование [24] оценивает несколько методов машинного обучения, включая SVM и наивный байесовский алгоритм, улучшенные с помощью метода n-грамм, помогающего захватывать последовательность символов в скриптах для улучшения производительности обнаружения. Указывается, что эффективность данного подхода была протестирована в реальных сценариях и позволяет достигать точности обнаружения в 98 %.

2. **Гибридные модели машинного обучения.** Использование гибридных моделей, таких как комбинация CNN и методов машинного обучения, позволяет эффективно выявлять XSS-атаки. Например, в исследовании [25] предложена модель, которая сочетает CNN и LSTM для повышения точности обнаружения XSS-атак. CNN используется для извлечения признаков из входных данных, а LSTM помогает анализировать временные зависимости и контекстуальные семантики. Это позволяет системе более точно идентифицировать вредоносные скрипты, даже если они замаскированы под легитимные запросы.

3. **Глубокое обучение.** В исследовании [26] изучается использование моделей глубокого обучения, таких как CNN и LSTM, которые могут фиксировать как пространственные, так и временные характеристики веб-запросов. А в исследовании [27] для улучшения обнаружения XSS-атак используются гибридные семантические вложения. Объединяя семантический анализ с традиционным машинным обучением, эти модели могут лучше понимать намерения, стоящие за веб-запросами, что приводит к улучшению показателей обнаружения.

4. **Использование векторизации и алгоритмов машинного обучения.** Применение TF-IDF векторизации и One Class SVM для обнаружения XSS-атак позволяет эффективно выявлять аномалии без необходимости включения данных об атаках в обучающую выборку [28]. Этот подход помогает преобразовать текстовые данные в числовые векторы, что облегчает их анализ. В свою очередь, One Class SVM обучается на нормальных данных и выявляет отклонения, которые могут указывать на наличие XSS-атак. Этот метод особенно полезен в условиях, когда данные об атаках ограничены или отсутствуют, так как он позволяет выявлять новые и неизвестные угрозы.

5. **Глубокое обучение и нейронные сети.** Использование глубоких нейронных сетей, таких как LSTM, для анализа временных зависимостей и контекстуальных семантик в XSS-пейлоудах позволяет улучшить обнаружение и предотвращение XSS-атак [29]. LSTM способны учитывать последовательность символов и их взаимосвязь, что делает их эффективными для анализа сложных текстовых данных. Это особенно важно для XSS-атак, где вредоносный код может быть замаскирован под легитимные запросы. Глубокое обучение позволяет системе адаптироваться к новым типам атак и улучшать свои модели на основе полученных данных.

6. **Модели на основе генеративных сетей.** Применение генеративных моделей помогает создавать синтетические данные для обучения систем обнаружения XSS-атак, что особенно полезно в условиях ограниченных данных, так как позволяет расширить обучающую выборку и улучшить точность обнаружения. Например, в исследовании [30] изучается использование GAN для создания состязательных XSS-атак, повышающих надёжность систем обнаружения. В работе [31] исследуются такие генеративные сети, как Wasserstein GAN с градиентным штрафом, авторы приходят к выводу об их высокой эффективности.

7. **Интеграция с существующими системами безопасности.** Внедрение ИИ в существующие системы безопасности, такие как межсетевые экраны и системы предотвращения вторжений, позволяет автоматизировать процессы обнаружения и реагирования на XSS-атаки [32]. ИИ может анализировать сетевой трафик в реальном времени, выявлять аномалии и автоматически блокировать подозрительные запросы. Это повышает общую эффективность защиты и снижает количество ложных срабатываний. Интеграция ИИ с существующими системами также позволяет улучшить их адаптивность и способность реагировать на новые угрозы.

8. **Графовые свёрточные сети (GCN).** Обеспечивают более полное понимание потенциальных угроз. В работе [33], посвящённой использованию GCN для обнаружения XSS, предлагается модель, которая эффективно идентифицирует полезные нагрузки XSS, используя графовые признаки, что фиксирует отношения между различными частями веб-запроса, обеспечивая более полное понимание потенциальных угроз.

2.2. Возможности использования ИИ в области предотвращения XSS-атак

Представленные ниже стратегии демонстрируют, как ИИ может быть использован в области предотвращения XSS-атак.

1. **Методы контролируемого обучения.** Модели машинного обучения, такие как метод опорных векторов и наивный байесовский алгоритм, используются для классификации и предотвращения атак XSS. Эти модели обучаются на наборах данных, содержащих как безвредные, так и вредоносные скрипты, что позволяет им распознавать и блокировать потенциальные угрозы [34].

2. **Глубокое обучение.** В работе [35] рассматривались возможности модели глубокого обучения, такие как LSTM-Attention, для обнаружения атак XSS с фокусом на критических частях входных данных, что позволяет предотвращать достаточно сложные атаки.

3. **Гибридные модели машинного обучения.** Использование гибридных моделей, таких как комбинация CNN и методов машинного обучения, позволяет эффективно выявлять XSS-атаки. Эти модели обучаются на больших наборах данных, что повышает их точность и устойчивость к новым типам атак [26].

4. **Использование генеративных моделей.** Применение генеративных моделей, таких как Wasserstein GAN с градиентным штрафом, помогает создавать синтетические данные для обучения систем обнаружения XSS-атак. Это особенно полезно в условиях ограниченных данных, что позволяет улучшить точность обнаружения [36].

5. **Интеграция с существующими системами безопасности.** Внедрение ИИ в существующие системы безопасности, такие как межсетевые экраны и системы предотвращения вторжений, позволяет автоматизировать процессы обнаружения и реагирования на XSS-атаки. Это повышает общую эффективность защиты и снижает количество ложных срабатываний [37]. При этом такие системы могут учиться на моделях трафика и адаптироваться к новым угрозам, обеспечивая динамический механизм защиты.

6. **Обучение на основе естественного языка.** Применение моделей обработки естественного языка, таких как BERT и BiLSTM, для извлечения и анализа текстовых данных помогает более эффективно выявлять вредоносные скрипты и предотвращать XSS-атаки [38].

2.3. Возможности использования ИИ в области реагирования на XSS-атаки

Системы с использованием ИИ могут автоматически реагировать на атаки XSS в реальном времени, что позволяет смягчить атаки до того, как они смогут причинить вред. Интегрируя ИИ в механизмы реагирования на XSS-атаки, организации могут значительно повысить свои возможности по смягчению этих угроз.

1. **Динамическая фильтрация контента.** Инструменты на основе ИИ могут динамически фильтровать и очищать веб-контент, чтобы предотвратить выполнение вредоносных скриптов. Это включает анализ входящих данных и их изменение для удаления потенциально опасных элементов до того, как они попадут к пользователю [39].

2. **IDS-системы с использованием ИИ.** Модели ИИ могут быть интегрированы с существующими IDS для улучшения их возможностей обнаружения и реагирования. Используя алгоритмы машинного обучения, эти системы могут лучше определять аномальное поведение, указывающее на попытки

XSS-атак, и запускать соответствующие ответы, а также производить оценку эффективности реагирования и обновления моделей обнаружения на основе новых идей [40].

3. **Адаптивное обучение и реагирование.** Системы ИИ могут адаптироваться к новым шаблонам атак, постоянно обучаясь на обнаруженных угрозах. Эта адаптивная способность позволяет совершенствовать стратегии реагирования, гарантируя, что система остаётся эффективной против развивающихся методов XSS-атак [41].

3. Возможности ИИ в обнаружении, предотвращении и реагирования на CSRF-атаки

CSRF (Cross-Site Request Forgery) — это тип кибератаки, в которой злоумышленник обманом заставляет пользователя выполнить нежелательные действия на веб-сайте, на котором он аутентифицирован. Эта атака эксплуатирует доверие веб-приложения к аутентифицированным пользователям, отправляя запросы от их имени, что может привести к нежелательным изменениям в данных или настройках. Искусственный интеллект может помочь в противодействии CSRF-атакам, включая их обнаружение, предотвращение и реагирование на них.

3.1. Возможности использования ИИ в области обнаружения CSRF-атак

Методы обнаружения на основе ИИ позволяют повысить эффективность обнаружения этих атак, используя сильные стороны машинного обучения и расширенного анализа данных для обеспечения надёжной защиты от развивающихся угроз.

1. **Использование алгоритмов машинного обучения.** Использование алгоритмов машинного обучения позволяет, в том числе, проводить анализ исторических данных о трафике и выявления признаков CSRF-атак. Так, в работе [42] предложено использование методов кластеризации и классификации для идентификации подозрительных запросов.

2. **Графовый анализ.** Например, в работе [43] исследовалась эффективность использования для обнаружения CSRF-уязвимостей графового анализа. Исследования показали высокую эффективность использования таких моделей.

3. **Методы ансамблевого обучения.** Например, в [44] исследуются ансамблевые модели Extreme Gradient Boosting и Extra Trees. На наш взгляд, их производительность позволит обеспечить высокую эффективность при выявлении CSRF-атак.

3.2. Возможности использования ИИ в области предотвращения CSRF-атак

В области предотвращения CSRF-атак применение ИИ также позволяет повысить эффективность решений и их адаптивность к новым угрозам.

1. **Самообучающиеся системы.** Разработка интеллектуальных систем, которые могут адаптироваться к новым угрозам и автоматически обновлять свои модели обнаружения. Такие системы могут использоваться для постоянного мониторинга и анализа сетевого трафика, что позволяет своевременно выявлять и блокировать попытки CSRF-атак [45].

2. **Интеграция с существующими системами безопасности.** ИИ может быть интегрирован с существующими системами безопасности для улучшения их эффективности. Это включает в себя использование ИИ для автоматизации процессов реагирования на инциденты и улучшения точности обнаружения угроз [46].

3. **Разработка гибких стратегий.** Использование ИИ для разработки стратегий, которые могут адаптироваться к изменяющимся условиям и новым типам атак. Это может включать в себя использование гибридных моделей, которые комбинируют различные подходы к обнаружению и предотвращению атак [46].

4. **Использование алгоритмов машинного обучения для поведенческого анализа.** Системы ИИ могут анализировать поведение пользователя и шаблоны запросов для обнаружения аномалий, которые могут указывать на атаку CSRF. Это включает в себя мониторинг необычной активности, которая отклоняется от обычных взаимодействий пользователя. Исследование [42] демонстрирует эффективность использования машинного обучения для анализа взаимодействий пользователя и атрибутов сеанса в режиме реального времени.

5. **Использование алгоритмов машинного обучения для анализа трафика.** Модели машинного обучения можно использовать для анализа веб-трафика и выявления запросов, не имеющих анти-CSRF-токенов. Например, в работе [46] предлагается метод пассивного обнаружения CSRF-устойчивых запросов путем анализа шаблонов трафика с использованием алгоритмов машинного обучения.

6. **Интеграция ИИ с сетевыми экранами.** ИИ может улучшить возможности брендмауэров, предоставляя интеллектуальную фильтрацию и блокировку вредоносных запросов. Эта интеграция позволяет более точно обнаруживать и предотвращать CSRF атаки, используя способность ИИ к обучению и адаптации к новым угрозам [46].

3.3. Возможности использования ИИ в области реагирования на CSRF-атаки

Решения на основе ИИ позволяют обеспечить возможности динамического реагирования в реальном времени.

1. **Обнаружение и смягчение в реальном времени.** Системы ИИ могут автоматически обнаруживать и реагировать на атаки CSRF в реальном времени.

Используя модели машинного обучения, эти системы могут быстро идентифицировать подозрительные запросы и применять контрмеры для предотвращения несанкционированных действий [39]

2. **Интеграция ИИ с IDS.** Модели ИИ могут быть интегрированы с существующими IDS для улучшения их возможностей обнаружения и реагирования. Используя алгоритмы машинного обучения, эти системы могут лучше идентифицировать аномальное поведение, указывающее на попытки CSRF, и инициировать соответствующие ответы [23].

3. **Использование машинного обучения для анализа и обучения после атаки.** После атаки системы ИИ могут анализировать инцидент, чтобы выявлять уязвимости и улучшать будущие стратегии реагирования. Это включает оценки эффективности реагирования и обновления моделей обнаружения на основе новых идей [46].

4. Проблемы использования ИИ в кибербезопасности и направления будущих исследований

В качестве основных проблем использования ИИ в кибербезопасности можно выделить:

- **Обучение на ограниченных данных.** Для эффективного обучения моделей ИИ требуется большое количество данных. Однако в кибербезопасности часто наблюдается нехватка данных о реальных атаках, что затрудняет обучение и тестирование моделей.

- **Адаптация к новым угрозам.** Киберугрозы постоянно эволюционируют, и модели ИИ должны быстро адаптироваться к новым типам атак. Это требует постоянного обновления и дообучения моделей, что может быть ресурсозатратным процессом.

- **Этичность и конфиденциальность.** Использование ИИ в кибербезопасности поднимает вопросы этичности и конфиденциальности, особенно в контексте обработки персональных данных. Необходимо разрабатывать методы, которые обеспечивают защиту данных пользователей.

В то же время, на наш взгляд, указанные ниже направления исследований помогут преодолеть существующие проблемы и расширить возможности применения ИИ в кибербезопасности, обеспечивая более надежную защиту информационных систем:

- **Разработка устойчивых моделей.** Исследования должны быть направлены на создание моделей, которые могут эффективно работать в условиях ограниченных данных и адаптироваться к новым угрозам. Это может включать использование методов переноса обучения и генеративных моделей.

- **Интеграция с другими технологиями.** Будущее развитие может включать интеграцию ИИ с другими технологиями, такими как блокчейн и квантовые вычисления, для создания более комплексных систем защиты.
- **Улучшение интерпретируемости моделей.** Для повышения доверия к ИИ-системам необходимо разрабатывать методы, которые делают модели более интерпретируемыми и прозрачными для пользователей и специалистов по безопасности.
- **Этические и правовые аспекты.** Необходимо продолжать исследования в области этических и правовых аспектов использования ИИ в кибербезопасности, чтобы обеспечить соблюдение прав пользователей и защиту их данных.

Заключение

Таким образом, можно сделать вывод, что применение ИИ в сфере кибербезопасности предоставляет значительные преимущества, включая автоматизацию процессов, повышение точности и адаптивность к новым угрозам. При этом следует отметить, что технологии ИИ продолжают развиваться, предлагая всё новые возможности для обеспечения кибербезопасности.

Литература

1. Crowdstrike 2024 Global Threat Report. URL: `https://go.crowdstrike.com/global-threat-report-2024.html` (дата обращения: 18.10.2024).
2. Hacham S.A.K., UÇan O.N. Detection of Malicious SQL Injections Using SVM and KNN Algorithms // 2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS). Istanbul, 2023. P. 1–5.
3. Angula T.J., Hashiyana V. Detection of Structured Query Language Injection Attacks Using Machine Learning Techniques // International Journal of Computer Science and Information Technology (IJCSIT). 2023. Vol. 15, No. 4.
4. Recio-Garcia J.A., Orozco-Del-Castillo M.G., Soladrero J.A. Case-based Explanation of Classification Models for the Detection of SQL Injection Attacks // CEUR Workshop Proceedings. 2023. Vol. 3438. P. 200–215.
5. Ibrohim M.M., Suryani V. Classification of SQL Injection Attacks using ensemble learning SVM and Naïve Bayes // International Conference on Data Science and Its Applications (ICoDSA). IEEE, 2023. P. 230–236.
6. Farooq U. Ensemble machine learning approaches for detection of SQL injection attack // Tehnički glasnik. 2021. Vol. 15, No. 1. P. 112–120.
7. Alghawazi M., Alghazzawi D., Alarifi S. Deep learning architecture for detecting SQL injection attacks based on RNN autoencoder model // Mathematics. 2023. Vol. 11, No. 15. Art. 3286.
8. Luo A., Huang W., Fan W. A CNN-based Approach to the Detection of SQL Injection Attacks // IEEE/ACIS 18th International Conference on Computer and Information Science (ICIS). IEEE, 2019. P. 320–324.
9. ALAzzawi A. SQL Injection Detection Using RNN Deep Learning Model // Journal of Applied Engineering and Technological Science (JAETS). 2023. Vol. 5, No. 1. P. 531–541.

10. Gandhi N., Patel J., Sisodiya R., Doshi N., Mishra S. A CNN-BiLSTM based approach for detection of SQL injection attacks // International conference on computational intelligence and knowledge economy (ICCIKE). IEEE, 2021. P. 378–383.
11. Li Y., Zhang B. Detection of SQL injection attacks based on improved TFIDF algorithm // Journal of Physics: Conference Series. 2019. Vol. 1395, No. 1. Art. 012013.
12. Venkatramulu S., Waseem M.S., Taneem A., Thoutam S.Y., Apuri S. Research on SQL injection attacks using word embedding techniques and machine learning // Journal of Sensors, IoT and Health Sciences. 2024. Vol. 2, No. 1. P. 55–66.
13. Lu D., Fei J., Liu L., Li Z. A GAN-based method for generating SQL injection attack samples // IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC). IEEE, 2022. Vol. 10. P. 1827–1833.
14. Li Q., Li W., Wang J., Cheng M. A SQL injection detection method based on adaptive deep forest // IEEE Access. 2019. Vol. 7. P. 145385–145394.
15. Coscia A., Dentamaro V., Galantucci S., Maci A., Pirlo G. PROGESI: a PROxy Grammar to Enhance web application firewall for SQL Injection prevention // IEEE Access. 2024.
16. Maina H.Y. A Critical Evaluation of Security Approaches for Detection and Prevention of SQL Injection Attacks in Web-Based Applications // FUDMA Journal of Sciences. 2024. Vol. 8, No. 2. P. 241–246.
17. Nair S.S. Securing Against Advanced Cyber Threats: A Comprehensive Guide to Phishing, XSS, and SQL Injection Defense // Journal of Computer Science and Technology Studies. 2024. Vol. 6, No. 1. P. 76–93.
18. Li Z., et al. LLM-Assisted Static Analysis for Detecting Security Vulnerabilities // ArXiv preprint. 2024. arXiv:abs/2405.17238.
19. Abdullah A.S., Shankar A.R., Mohapatra P. Detection and Analysis of Port Scanning and SQL Injection Vulnerabilities with correlating factors in Web Applications to Enhance secure Data Transmission // International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE). Chennai, India, 2023. P. 1–5.
20. Xu M., Xie B., Cui F., Jin C., Wang Y. SQL injection attack sample generation based on IE-GAN // IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2023. P. 1014–1021.
21. Irungu J., Graham S., Girma A., Kacem T. Artificial intelligence techniques for SQL injection attack detection // Proceedings of the 2023 8th International Conference on Intelligent Information Technology. 2023. P. 38–45.
22. Ashlam A.A., Badii A., Stahl F. Multi-Phase Algorithmic Framework to Prevent SQL Injection Attacks using Improved Machine learning and Deep learning to Enhance Database security in Real-time // 15th International Conference on Security of Information and Networks (SIN). Sousse, Tunisia, 2022. P. 1–4.
23. Gaspar D., Silva P., Silva C. Explainable AI for Intrusion Detection Systems: LIME and SHAP Applicability on Multi-Layer Perceptron // IEEE Access. 2024. Vol. 12. P. 30164–30175.
24. Upender T., Lal B., Nagaraju R. Transfer Learning Method for Handling The Intrusion Detection System with Zero Attacks Using Machine Learning and Deep Learning // Proceedings of the 5th International Conference on Information Management and Machine Intelligence. 2023. P. 1–11.
25. Lente C., et al. An Improved Tool for Detection of XSS Attacks by Combining CNN with LSTM // Anais Estendidos do XXI Simpósio Brasileiro de Segurança da Informação e de

Sistemas Computacionais (SBSeg Estendido 2021). 2021.

26. Abhishek S., et al. AI-Driven Deep Structured Learning for Cross-Site Scripting Attacks // International Conference on Innovative Data Communication Technologies and Application (ICIDCA). Uttarakhand, India, 2023. P. 701–709.
27. Bakır Ç. New Hybrid Distributed Attack Detection System for IoT // Bitlis Eren Üniversitesi Fen Bilimleri Dergisi. 2024. Vol. 13, No. 1. P. 232–246.
28. Tamamura K., Sakai S., Watarai K., Okada S., Mitsunaga T. Detection of XSS Attacks with One Class SVM Using TF-IDF and Devising a Vectorized Vocabulary // IEEE International Conference on Computing (ICOCO). IEEE, 2023. P. 35–40.
29. Et-Tolba M., et al. DL-Based XSS Attack Detection Approach Using LSTM Neural Network with Word Embeddings // 11th International Conference on Wireless Networks and Mobile Communications (WINCOM). 2024. P. 1–6.
30. Alhamyani R., Alshammari M. Machine Learning-Driven Detection of Cross-Site Scripting Attacks // Information. 2024. Vol. 15. No. 7. P. 420. DOI: 10.3390/info15070420.
31. Mokbal F.M.M., Wang D., Wang X., Fu L. Data augmentation-based conditional Wasserstein generative adversarial network-gradient penalty for XSS attack detection system // PeerJ Computer Science. 2020. Vol. 6. Art. e328.
32. Hubballi N., et al. XSSMitigate: Deep Packet Inspection based XSS Attack Quarantine in Software Defined Networks // IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2023. Art. 1025.
33. Liu Z., Fang Y., Huang C., Han J. GraphXSS: An efficient XSS payload detection approach based on graph convolutional network // Computers and Security. 2022. Vol. 114. Art. 102597.
34. Kaur J., Garg U., Bathla G. Detection of cross-site scripting (XSS) attacks using machine learning techniques: a review // Artificial Intelligence Review. 2023. Vol. 56. P. 12725-–12769.
35. Lei L., Chen M., He C., Li D. XSS Detection Technology Based on LSTM-Attention // 5th International Conference on Control, Robotics and Cybernetics (CRC). Wuhan, China, 2020. P. 175–180.
36. Oladiipo O.S., et al. AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection // Asian Journal of Research in Computer Science. 2024.
37. Wang Q., Huang J., Qi X. XSS attack detection and prevention system based on instruction set randomization // IOP Conference Series: Materials Science and Engineering. 2019. Vol. 563, No. 4. Art. 042086.
38. Wan S., Xian B., Wang Y., Lu J. Methods for Detecting XSS Attacks Based on BERT and BiLSTM // 8th International Conference on Management Engineering, Software Engineering and Service Sciences (ICMSS). IEEE, 2024. P. 1–7.
39. Shahid M. Machine learning for detection and mitigation of web vulnerabilities and web attacks. ArXiv preprint. 2023. arXiv:2304.14451.
40. Ahmed Mohanad Jaber ALHILO, Hakan Koyuncu. Enhancing SDN Anomaly Detection: A Hybrid Deep Learning Model with SCA-TSO Optimization // International Journal of Advanced Computer Science and Applications. 2024. Vol. 15, No. 5.
41. Shradha F., et al. Detection of cyber-attacks and network attacks using Machine Learning // World Journal of Advanced Engineering Technology and Sciences. 2024.
42. Ramadan M., Osama B., Zaher M., Mansour H., El Sersi W. Enhancing Web Security: A Comparative Analysis of Machine Learning Models for CSRF Detection // Intelligent Methods, Systems, and Applications (IMSA). Giza, Egypt, 2024. P. 18–25.
43. Liu C., Shen X., Gao M., Dai W. CSRF Detection Based on Graph Data Mining // 2020

IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE). Dalian, China, 2020. P. 475–480.

44. Kharwar A.R., Thakor D.V. An Ensemble Approach for Feature Selection and Classification in Intrusion Detection Using Extra-Tree Algorithm // International Journal of Information Security and Privacy. 2022. Vol. 16, No. 1. P. 1–21.
45. Hadavi M.A., Sadeghi S. Automatic Black-Box Detection of Resistance Against CSRF Vulnerabilities in Web Applications // Journal of Computing and Security. 2021. Vol. 8, No. 1. P. 19–32.
46. Ghumman S. A Comparative Evaluation of network Attack Detection and Prevention Strategies in multi model Cloud servers // 4th IEEE Global Conference for Advancement in Technology (GCAT). 2023. P. 1–6.

AI CAPABILITIES IN CYBERSECURITY: DETECTION, PREVENTION AND RESPONSE TO SQL INJECTIONS, XSS, AND CSRF ATTACKS

D.E. Vilkhovsky
Assistant Professor, e-mail: vilkhovskiy@gmail.com

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The paper provides an overview of the possibilities of using artificial intelligence to enhance the cybersecurity of web applications, with an emphasis on detecting, preventing, and responding to SQL injections, XSS, and CSRF attacks. Machine learning methods such as SVM, Naive Bayes, ensemble learning, and deep learning are discussed, as well as their integration with existing security systems. Hybrid models and approaches to adapting systems to new threats are included. Existing problems are analyzed and future research directions for overcoming these challenges are identified

Keywords: computer security, information security, cybersecurity, SQL injections, XSS attacks, CSRF attacks, machine learning, artificial intelligence.

Дата поступления в редакцию: 20.10.2024