БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2021. – № 3 (102). – 57–67

УДК 004.85 DOI: 10.17212/2782-2230-2021-3-57-67

АНАЛИЗ ОБНАРУЖЕНИЯ АТАКИ НА БАЗЕ SQL-ИНЪЕКЦИИ С ПОМОЩЬЮ ИМПУЛЬСНОЙ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ*

А.Б. АРХИПОВА[1], П.А. ПОЛЯКОВ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент кафедры защиты информации. E-mail: arhipova@corp.nstu.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: ctf@corp.nstu.ru*

В настоящей статье представлены результаты тестирования по созданию специализированной системы, которая помогает предотвратить кибератаки и таким образом популяризирует построение интеллектуальных приложений. По полученным результатам можно утверждать, что проведенные испытания являются удовлетворительными. Математической основой построения нейросетевой модели является модель HESADM (Hybrid Artificial Intelligence Framework). Представленная система позволяет формировать набор правил с помощью нечетких логических нейронов. В настоящей работе представлен подход к формированию нечеткой нейронной сети, используемой при обнаружении атак SQL-инъекций. Методология, использованная в настоящей работе, представляет собой импульсную искусственную нейронную сеть (SANN), которая использует эволюционирующая нейросетевую систему (eCOS) и многослойный подход импульсной искусственной нейронной сети для классификации точного типа вторжения или сетевой аномалии с минимальным вычислительным потенциалом. Импульсная искусственная нейронная система формирует себя непрерывно, адаптируясь к входным данным, будучи в функционирующем или нефункционирующем состоянии, находясь под наблюдением администратора. Данная система находит применение к нескольким другим сложным проблемам реального мира, тем самым доказывает свою работоспособность, в том числе в области информационной безопасности. Рассмотренная модель представляет собой гибридную эволюционирующую импульсную модель обнаружения аномалии (HESADM), которая работает на импульсах, возникающих в системе, в то время как нейроны применяются для мониторинга алгоритма с использованием одного прохода обучения. В системе трафик-ориентированные данные применяют путем импорта классов, которые используют переменное кодирование. Используемые данные получены путем преобразования реальных характеристик сетевого трафика в определенные временные отметки.

* Статья получена 20 июня 2021 г.

Ключевые слова: кибератаки, информационная безопасность, импульсная искусственная нейронная сеть, нейронная агрегационная сеть, атаки SQL-инъекций, модель обнаружения кибератак, система нечеткого вывода, функция принадлежности

ВВЕДЕНИЕ

В мировой ситуации киберпространство – это область, в которой, несмотря на понимание необходимости обеспечения безопасности, нет никаких систематических и четко сформулированных мер, которые могли бы гарантировать надежность и сохранность используемых систем. Основной целью развития общества с этих позиций является минимизация количества кибератак на сети и государственные информационные системы, а также на все другие сегменты общества [11]. В последнее время всё большее внимание уделяется кибербезопасности как стратегической функции государства, так как она имеет важное значение для поддержания критически важных инфраструктур страны. Другими словами, в контексте цифрового развития государства ни одна страна не может отказаться от безопасности своего киберпространства.

На сегодняшний день атаки на информационные системы компании являются куда более сложными и требуют специальных средств защиты, особенно для объектов критических информационных инфраструктур. Стоит отметить, что с учетом увеличения количества информационных потоков и разновидностей их использования уровень угроз информационной безопасности объектов критических информационных инфраструктур значительно возрастает. Анализ показал отсутствие комплексного подхода к предотвращению угроз информационной безопасности. В этой связи важное значение приобретают нейронные сети, которые используют повсеместно, например, при сравнении биометрических характеристик человека [5, 8], в юриспруденции [7], банковской сфере [9], информационной безопасности [1, 2, 7, 10–15], медицине и биологии [4] и т. п. [6] Методология, использованная в данной работе – это импульсная искусственная нейронная сеть, которая использует эволюционирующую нейросетевую систему и многослойный подход для классификации точного типа вторжения или сетевой аномалии с минимальным вычислительным потенциалом.

1. СХЕМА АТАКИ НА БАЗЕ SQL-ИНЪЕКЦИИ

Язык структурированных запросов, или SQL, является языком по умолчанию для взаимодействия с реляционными базами данных. В нем выполняются основные задачи, связанные с манипулированием данными в структурах баз

данных [14]. SQL-инъекция – это тип кибератаки, которая использует ошибки в системах, обычно имеющие связь с базой данных через SQL-команды, и по этой причине считается разновидностью атаки прямолинейной. В этом процессе вторжения злоумышленник может вставить пользовательскую и ненужную инструкцию SQL в запрос через формы записи данных программы. В полях, предназначенных для информации пользователя, эти команды выполняются, т. е. отображаются команды SQL, однако из-за этого сбоя в приложениях они в конечном итоге вызывают изменения в базе данных или неправильный доступ к приложению [14]. Взломщик может получить любые скрытые данные, хранящиеся в базе данных серверного компьютера, с помощью SQL-инъекционных атак, в том числе в зависимости от версии базы данных. Вы также можете вводить вредоносные команды и получать полное разрешение на машину, на которой работает банк [9]. На рис. 1 показаны основные шаги для атаки с помощью SQL-инъекции.

Рис. 1. Схематическое представление атаки, основанной на SQL-инъекции

Fig. 1. Schematic representation of an attack based on SQL injection

2. МЕТОДОЛОГИЯ ОБНАРУЖЕНИЯ АТАКИ

В статье «Обнаружение сетевых аномалий на основе эволюции нейронных сетей», написанной К. Демерцисом и Л. Илиадисом [1], описывается интеллектуальная система машинного обучения, где часть системы работает в

поисках известных угроз, а другая часть пытается обнаружить вероятные угрозы в соответствии с аномальными действиями, которые происходят в штатном порядке. Система обнаружения проста, она генерирует состояние, обрабатываемое как обычно, и все сигналы за пределами края этого состояния обрабатываются как аномалия, поэтому алгоритм обнаружения учится непрерывно, пока система активна в сети.

Методология, использованная в настоящей работе, – это импульсная искусственная нейронная сеть (ИНС) (SANN), которая использует эволюционирующую нейросетевую систему (eCOS) и многослойный подход ИНС для классификации точного типа вторжения или сетевой аномалии с минимальным вычислительным потенциалом; SANN – это набор модульных систем, основанных на узловых соединениях. Система формирует себя непрерывно, адаптируясь к входным данным, будучи в функционирующем или нефункционирующем состоянии, находясь под наблюдением администратора. SANN также применяется к нескольким другим сложным проблемам реального мира, доказывая свою работоспособность. Разработанная модель называется гибридной эволюционирующей импульсной моделью обнаружения аномалии (HESADM), которая работает на импульсах, возникающих в системе, в то время как нейроны используются для мониторинга алгоритма с использованием одного прохода обучения.

Трафик-ориентированные данные используются путем импорта классов, которые используют переменное кодирование всего множества данных. Используемые данные получены путем преобразования реальных характеристик сетевого трафика в определенные временные отметки. Данные были классифицированы на два типа:

1) класс 0, соответствующий нормальным, штатным результатам;

2) класс 1, соответствующий аномальным результатам.

Во время верификации атаки, если результат равен нулю, процесс классификации eSNN повторяется, но с соответствующими обновленными векторами данных. Если результат продолжает равняться нулю, процесс завершается. Когда результатом является класс 1, нейронная сеть из двух слоев используется для распознавания типа атаки и использует все ресурсы базы данных KDD и NSL-KDD [1]. Если это происходит в скрытом слое, используются 33 нейрона. Результаты этого процесса представляются сетевому администратору в виде предупреждения, графическая модель HESADM показана на рис. 2 [1].

Для обучения и тестов были выбраны два набора данных: KDD и NSL-KDD.

KDD-коллекция содержит данные, имитирующие сеть. Метод анализа событий включает в себя соединение между IP-адресом источника и IP-адресом

назначения, во время которого происходит обмен последовательностью TCP-пакетов, использующих определенный протокол и строго определенное время работы. Используемая база данных включает в себя список из 13 884 SQL-операторов, выбранных различными источниками; 12 881 из них являются вредоносными (SQL-инъекции), а 1003 – законными (корреляция SQL-операторов с типом SQL-инъекций).

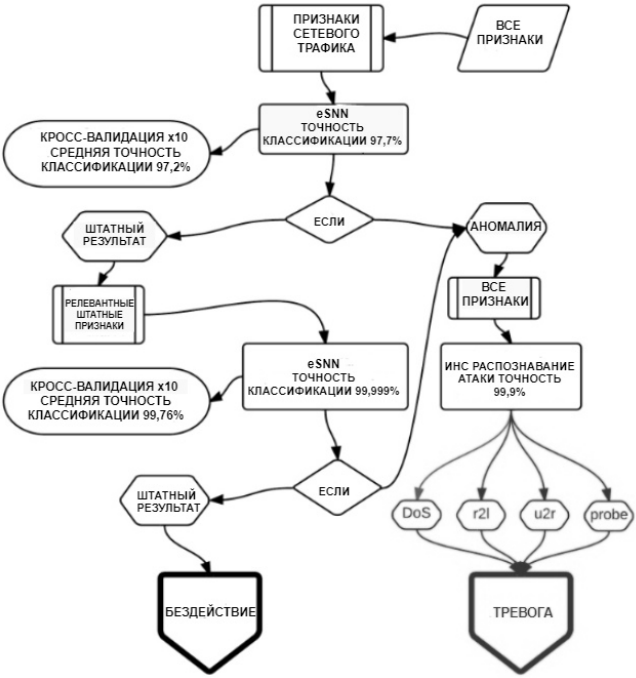

Рис. 2. Модель HESADM

Fig. 2. Model HESADM

NSL-KDD – это набор данных, предложенный для решения некоторых внутренних проблем набора данных KDD'99, которые упоминаются в работе [10]. Усовершенствованная коллекция применяется в качестве эффективного эталонного набора данных для разработки методов обнаружения вторжений с помощью различных сетевых атак. В таблице показана отличная производительность и надежность схемы, предложенной в работе [1]. В ней представлены результаты категоризации с использованием одного и того же набо-

ра данных SQL-инъекций, 10-кратной перекрестной проверки и других подходов машинного обучения, модель достигла результата 99,6 %.

Точность работы различных классификаторов

The accuracy of the various classifiers

Классификатор	Точность, %
MFF ANN с GA	99.6
RBFNetwork	97.3
NaiveBayes	98.7
SVM	98.5
k-NN	98.3
Random Forest	99.1

ЗАКЛЮЧЕНИЕ

Для выполнения тестов обнаружения атак и создания экспертной системы, основанной на характере данных, были использованы описанные ранее базы данных KDD'99 и NSL-KDD. Несбалансированные наборы данных являются частным случаем проблем классификации, когда распределение классов неоднородно, что наблюдается в KDD'99. Обычно подобные классы делятся на две категории: большинство (отрицательные) и меньшинство (положительные).

Из всех характеристик, предложенных в указанных наборах данных, были использованы параметры: длина, энтропия, уровень агрессивности, уровень доверия и уверенности. Экспертная система основана на правилах «ЕСЛИ» и «ТО». Нечеткие нейронные сетевые модели (UNI-RNN – это нечеткая нейронная сеть, состоящая из унинейронов, а AND-RNN – из анднейронов) были сопоставлены с другими алгоритмами классификатора для базы данных: SVM, MLP, NBCи C4.5.

Для визуализации работы алгоритмов интеллектуального анализа данных возможно использование набора инструментов weka [10]. Его конфигурации и использование основаны на работе [1].

Следует отметить, что во избежание тенденций в проведенных испытаниях был проведен обмен всеми имеющимися образцами и было собрано 30 измерений точности с каждой из баз, оцененных в каждой анализируемой модели. Переменные, участвующие в этом процессе, были нормализованы со средним нулем и дисперсией 1. Все атаки SQL-инъекций модели были нормализованы к интервалу [–1, 1].

Для нечеткой нейросетевой модели оптимальные параметры M, b и p найдены путем перекрестной валидации (70 % обучения, 30 % для тестирования) с использованием 10-кратного метода. Диапазоны были следующими: $M = \{2, 3, 4\}$, $b = \{8, 16, 32\}$, $\rho = \{50\ \%, 60\ \%, 70\ \%\}$. Значение L_c было оценено на уровне 200, как и в [10]. Результаты были представлены тестами, выполненными на персональном компьютере с процессором IntelCore i7-4700 MQ2,40 ГГц и памятью 8,00 ГБ.

Итоговая система представила полезные результаты по использованию нечетких правил для построения систем. Мы можем выделить пример, полученный при использовании двух функций принадлежности, позволяющих классифицировать параметры как низкие и высокие.

СПИСОК ЛИТЕРАТУРЫ

1. *Demertzis K., Iliadis L.* A bio-inspired hybrid artificial intelligence framework for cyber security // Computation, Cryptography, and Network Security. – Cham: Springer, 2015. – P. 161–193.

2. *Lighthil C.S.J.* Artificial intelligence: a paper symposium / Science Research Council. – 1973. – URL: http://www.chilton-computing.org.uk/inf/literature/reports/lighthill_report/p001.htm (accessed: 14.09.2021).

3. *Crevier D.* AI: the tumultuous search for artificial intelligence. – New York: Basic Books, 1993. – 203 p.

4. *Aceves-Fernandez M.A.* Artificial intelligence: applications in medicine and biology. – IntechOpen, 2019. – 140 p.

5. *Крохалева А.Б., Белов В.М.* Модели сравнения биометрических характеристик человека // Проблемы информационной безопасности государства, общества и личности: 16 международная научно-практическая конференция: доклады VII Пленума СибРОУМО и материалы XVI конференции, Томск, 6–10 июня 2018 г. – Томск : В-Спектр, 2018. – С. 48–52.

6. *Шмидт Э., Коэн Д.* Новый цифровой мир: как технологии меняют жизнь людей, модели бизнеса и понятие государств. – М.: Манн, Иванов и Фербер, 2013. – 368 с.

7. *Понкин И.В.*, *Редькина А.И.* Искусственный интеллект с точки зрения права // Вестник Российского университета дружбы народов. Серия: Юридические науки. – 2018. – № 1. – С. 91–109.

8. Artificial intelligence applications in civil engineering / T. Dede, M. Kankal, A.R. Vosoughi, M. Grzywiński, M. Kripka // Advances in Civil Engineering. – 2019. – Art. 8384523. – URL: https://www.hindawi.com/journals/ace/2019/8384523/ (accessed: 14.09.2021).

9. *Каблучко Ю.В.* Применение искусственного интеллекта в банковской сфере // Вопросы науки и образования. – 2018. – № 18. – С. 20–27.

10. The WEKA data mining software: an update / M. Hall, E. Frank, G. Holmes, B. Pfahringer, C. Reutemann, I.H. Witten // ACM SIGKDD Explorations Newsletter. – 2008. – N 11 (1). – P. 10–18.

11. *Foote K.D.* A brief history of machine learning. – 2019. – March 26. – URL: https://www.dataversity.net/a-brief-history-of-machine-learning/ (accessed: 14.09.2021).

12. *Russell S.J., Norvig C.* Artificial intelligence: a modern approach. – Englewood Cliffs, NJ: Prentice Hall, 1995. – 946 p.

13. *Noyes J.L.* Artificial intelligence with common lisp: fundamentals of symbolic and numeric processing. – Jones & Bartlett Learning, 1992. – 644 p.

14. Prevenção de ataques: XSS residente e SQL injectionem banco de dados PostgreSQL em ambiente WEB Estudos Tecnológicos / A. Vissotto Jr, E. Bosco, B.G. Bruschi, L.A. Silva // Caderno de Estudos Tecnológicos. – 2015. – Vol. 3, no. 1. – P. 38–50.

15. Cost-based modeling and evaluation for data mining with application to fraud and intrusion detection: results from the JAM project by Salvatore / J. Stolfo, W. Fan, W. Lee, A. Prodromidis, C.K. Chan // Proceedings DARPA Information Survivability Conference and Exposition, DISCEX'00. – 2000. – Vol. 2. – P. 130–144. – DOI: 10.1109/DISCEX.2000.821515.

Архипова Анастасия Борисовна, доцент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – математическое моделирование в информационной безопасности, оценка качества социально значимой деятельности. E-mail: arhipova@corp.nstu.ru

Поляков Павел Андреевич, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – математическое моделирование в информационной безопасности. E-mail: ctf@corp.nstu.ru

DOI: 10.17212/2782-2230-2021-3-57-67

Analysis of the detection of an attack based on SQL injection using an impulse artificial neural network*

A.B. Arkhipova[1], P.A. Polyakov[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, candidate of technical sciences, associate professor of the Department of Information Security. E-mail: arhipova@corp.nstu.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: ctf@corp.nstu.ru*

This article presents the results of testing to create a specialized system that helps prevent cyberattacks, thus popularizing the construction of intelligent applications. Based on the results obtained, it can be argued that the tests carried out are satisfactory. The mathematical basis for building a neural network model is the HESADM model (Hybrid Artificial Intelligence Framework). The presented system allows you to form a set of rules using fuzzy logical neurons. This paper presents an approach to the formation of a fuzzy neural network used for detecting SQL injection attacks. The methodology used in this paper is an impulse artificial neural network (SANN), which uses an evolving neural network system (eCOS) and a multi-layer approach of an impulse artificial neural network to classify the exact type of intrusion or network anomaly with minimal computational potential. The impulse artificial neural system forms itself continuously, adapting to the input data, being in a functioning or not state, being under the supervision of an administrator. This system finds application to several other complex problems of the real world, proving its efficiency, including in the field of information security. The considered model is a hybrid evolving pulse anomaly detection model (HESADM), which works on impulses that occur in the system, while neurons are used to monitor the algorithm using a single training pass. In the system, traffic-oriented data is used by importing classes that use variable encoding. The data used is obtained by converting the real characteristics of network traffic into certain time stamps.

Keywords: cyberattacks, information security, impulse artificial neural network, neural aggregation network, SQL injection attacks, cyberattack detection model, fuzzy inference system, membership function

REFERENCES

1. Demertzis K., Iliadis L. A bio-inspired hybrid artificial intelligence framework for cyber security. *Computation, Cryptography, and Network Security*. Cham, Springer, 2015, pp. 161–193.

2. Lighthil C.S.J. *Artificial intelligence: a paper symposium*. Science Research Council, 1973. Available at: http://www.chilton-computing.org.uk/inf/literature/reports/lighthill_report/p001.htm (accessed 14.09.2021).

* *Received 20 June 2021.*

3. Crevier D. *AI: the tumultuous search for artificial intelligence*. New York, Basic Books, 1993. 203 p.

4. Aceves-Fernandez M.A. *Artificial intelligence: applications in medicine and biology*. IntechOpen, 2019. 140 p.

5. Krokhaleva A.B., Belov V.M. [Models for comparing biometric characteristics of a person]. *Problemy informatsionnoi bezopasnosti gosudarstva, obshchestva i lichnosti*: 16 mezhdunarodnaya nauchno-prakticheskaya konferentsiya: doklady VII Plenuma SibROUMO i materialy XVI konferentsii [Problems of information security of the state, society and personality: XVI international scientific and practical conference], Tomsk, June 6–10, 2018, pp. 48–52. (In Russian).

6. Schmidt E., Cohen J. *Novyi tsifrovoi mir: kak tekhnologii menyayut zhizn' lyudei, modeli biznesa i ponyatie gosudarstv* [The new digital age: how technologies change people's lives, business models and the concept of states]. Moscow, Mann, Ivanov i Ferber Publ., 2013. 368 p. (In Russian).

7. Ponkin I.V., Red'kina A.I. Iskusstvennyi intellekt s tochki zreniya prava [Artificial intelligence from the point of view of law]. *Vestnik Rossiiskogo universiteta druzhby narodov. Seriya: Yuridicheskie nauki = RUDN Journal of Law*, 2018, no. 1, pp. 91–109.

8. Dede T., Kankal M., Vosoughi A.R., Grzywiński M., Kripka M. Artificial intelligence applications in civil engineering. *Advances in Civil Engineering*, 2019, art. 8384523. Available at: https://www.hindawi.com/journals/ace/2019/8384523/ (accessed 14.09.2021).

9. Kabluchko Yu.V. Primenenie iskusstvennogo intellekta v bankovskoi sfere [Application of artificial intelligence in the banking sector]. *Voprosy nauki i obrazovaniya = Questions of Science and Education*, 2018, no. 18, pp. 20–27.

10. Hall M., Frank E., Holmes G., Pfahringer B., Reutemann C., Witten I.H. The WEKA data mining software: an update. *ACM SIGKDD Explorations Newsletter*, 2008, no. 11 (1), pp. 10–18.

11. Foote K.D. *A brief history of machine learning*. 2019, March 26. Available at: https://www.dataversity.net/a-brief-history-of-machine-learning/ (accessed 14.09.2021).

12. Russell S.J., Norvig C. *Artificial intelligence: a modern approach*. Englewood Cliffs, NJ, Prentice Hall, 1995. 946 p.

13. Noyes J.L. *Artificial intelligence with common lisp: fundamentals of symbolic and numeric*. Jones & Bartlett Learning, 1992. 644 p.

14. Vissotto A. Jr, Bosco E., Bruschi B.G., Silva L.A. Prevenção de ataques: XSS residente e SQL injectionem banco de dados PostgreSQL em ambiente WEB Estudos Tecnológicos. *Caderno de Estudos Tecnológicos*, 2015, vol. 3, no. 1, pp. 38–50.

15. Stolfo S.J., Fan W., Lee W., Prodromidis A., Chan P.K. Cost-based modeling for fraud and intrusion detection: results from the JAM project. *Proceedings DARPA Information Survivability Conference and Exposition, DISCEX'00*, 2000, vol. 2, pp. 130–144. DOI: 10.1109/DISCEX.2000.821515.

Для цитирования:

Архипова А.Б., Поляков П.А. Анализ обнаружения атаки на базе SQL-инъекции с помощью импульсной искусственной нейронной сети // Безопасность цифровых технологий. – 2021. – № 3 (102). – С. 57–67. – DOI: 10.17212/2782-2230-2021-3-57-67.

For citation:

Arkhipova A.B., Polyakov P.A. Analiz obnaruzheniya ataki na baze SQL in"ektsii s pomoshch'yu impul'snoi iskus-stvennoi neironnoi seti [Analysis of the detection of an attack based on sql injection using an impulse artificial neural network]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2021, no. 3 (102), pp. 57–67. DOI: 10.17212/2782-2230-2021-3-57-67.