БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2021. – № 3 (102). – 43–56

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.85 DOI: 10.17212/2782-2230-2021-3-43-56

МЕТОДОЛОГИЯ ПОСТРОЕНИЯ НЕЙРОННОЙ НЕЧЕТКОЙ СЕТИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

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 работе предлагается использование гибридных моделей на основе нейронных сетей и нечетких систем для построения интеллектуальных систем обнаружения вторжения, основанных на теории нечетких правил. Представленная система сможет генерировать правила на основе результатов с использованием нечетких логических нейронов. Чтобы избежать перенасыщения и способствовать в определении необходимой топологии сети, обучающие модели, основанные на экстремальной обучающей машине и теории регуляризации, будут использоваться для поиска наиболее значимых нейронов. Рассмотрен тип кибератаки SQL-инъекция, которая активно использует ошибки в системах, имеющие связь с базой данных через SQL-команды, и по этой причине считается разновидностью прямолинейной атаки. Архитектура нечеткой нейронной сети, используемой при обнаружении атак SQL-инъекций, представляет собой многокомпонентную структуру. Первые два слоя модели рассматривают как систему нечеткого вывода, способную извлекать знания из данных и преобразовывать их в нечеткие правила. Эти правила помогают построить автоматизированные системы для обнаружения атак SQL-инъекций. Третий слой состоит из простого нейрона, который имеет функцию активации, называемую ReLU с утечкой. Первый слой состоит из нечетких нейронов, активационные функции которых являются гауссовыми функциями принадлежности нечетких множеств, определенных в соответствии с разбиением входных переменных. Методика использует понятие простой линейной регрессионной модели, позволяющей решить задачу выбора наилучших подмножеств нейронов. Для выполне-

* Статья получена 20 июня 2021 г.

ния выбора модели в статье был применен широко используемый алгоритм наименьшей угловой регрессии (LARS).

Ключевые слова: нечеткое множество, нечеткая нейронная сеть, информационная безопасность, нейронная агрегационная сеть, атаки SQL-инъекций значимых нейронов, модель обнаружения кибератак, система нечеткого вывода, функция принадлежности

ВВЕДЕНИЕ

С глобализацией и ростом зависимости общества от программных систем информация и данные, имеющие первостепенное значение для компаний и частных лиц по всему миру, мгновенно перемещаются через Интернет, привлекая внимание киберпреступников, когда они стремятся вторгнуться в системы или перехватить информацию для использования в своих интересах или во вред организациям, на которые они нападают, что делает последствия таких атак всё более влиятельными [3].

В настоящей работе предлагается использование гибридных моделей на основе нейронных сетей и нечетких систем для построения интеллектуальных систем обнаружения вторжения, основанных на нечетких правилах. Представленная система сможет генерировать правила на основе результатов с использованием нечетких логических нейронов. Чтобы избежать перенасыщения и поспособствовать в определении необходимой топологии сети, обучающие модели, основанные на экстремальной обучающей машине и теории регуляризации, будут использоваться для поиска наиболее значимых нейронов.

1. ПОНЯТИЕ НЕЧЕТКОЙ НЕЙРОННОЙ СЕТИ

Нейронная сеть – математическая модель, а также ее программное или аппаратное воплощение, построенные по принципу организации и функционирования биологических нейронных сетей – сетей нервных клеток живого организма [9].

Искусственные нейронные сети начинались как попытка использовать архитектуру человеческого мозга для выполнения задач, с которыми обычные алгоритмы не имели большого успеха. Вскоре они переориентировались на улучшение эмпирических результатов, в основном отказавшись от попыток оставаться верными своим биологическим предшественникам. Нейроны соединены друг с другом различными паттернами, чтобы выход одних нейронов стал входом для других. Сеть образует направленный, взвешенный граф.

Искусственные нейронные сети состоят из искусственных нейронов, которые сохраняют биологическую концепцию нейронов, получают входные данные, объединяют входные данные со своим внутренним состоянием (акти-

вацией) и дополнительным порогом с помощью функции активации, производят выходные данные с помощью функции вывода. Исходными данными являются внешние данные, такие как изображения и документы. Конечные результаты выполняют такую задачу, как, например, распознавание объекта в изображении. Важной характеристикой активационной функции является то, что она обеспечивает плавный дифференцируемый переход при изменении входных значений, т. е. небольшое изменение на входе приводит к небольшому изменению на выходе.

Искусственные нейронные сети широко применяются в различных областях. Так, например, современные компании применяют машинное обучение, чтобы ставить диагнозы лучше и быстрее, чем люди. Одна из самых известных медицинских технологий – IBM Watson. Она понимает естественный язык и может отвечать на вопросы, которые ему задают. Созданная система получает данные от пациентов и из прочих доступных источников для формирования гипотезы заболевания, которую затем проверяет с помощью схемы оценки достоверности. Целый ряд технологий искусственного интеллекта также используется для прогнозирования, борьбы и понимания пандемий, таких как COVID-19 [4–7, 9].

Алгоритмы машинного обучения интегрируются в платформы аналитики и управления взаимоотношениями с клиентами, чтобы выявить информацию о том, как лучше обслуживать клиентов. Чат-боты были включены в веб-сайты, чтобы обеспечить немедленное обслуживание клиентов. Автоматизация рабочих мест также стала предметом обсуждения среди ученых и IT-аналитиков [9].

Процесс изучения различных законов и прав часто является подавляющим для людей, но использование искусственного интеллекта для автоматизации трудоемких процессов юридической отрасли позволяет экономить время и улучшать обслуживание клиентов. Юридические фирмы используют машинное обучение для описания данных и прогнозирования результатов, компьютерное зрение для классификации и извлечения информации из документов и обработку естественного языка для интерпретации запросов на информацию [7].

2. МЕТОДОЛОГИЯ ПОСТРОЕНИЯ НЕЙРОННОЙ НЕЧЕТКОЙ СЕТИ

Модель обнаружения кибератак изначально была предложена для классификации бинарных паттернов. Эта модель представляет собой объединение понятий моделей, введенных в работах [10, 11]. На рис. 1 показана архитектура нечеткой нейронной сети, используемой при обнаружении атак SQL-инъекций. Первые два слоя модели рассматриваются как система нечеткого вывода, способная извлекать знания из данных и преобразовывать их в нечет-

кие правила. Эти правила помогают построить автоматизированные системы для обнаружения атак SQL-инъекций. По-разному рассмотренный в [10] третий слой состоит из простого нейрона, который имеет функцию активации по методике, предложенной в [12], называемой ReLU с утечкой.

Первый слой состоит из нечетких нейронов, активационные функции которых являются гауссовыми функциями принадлежности нечетких множеств, определенных в соответствии с разбиением входных переменных.

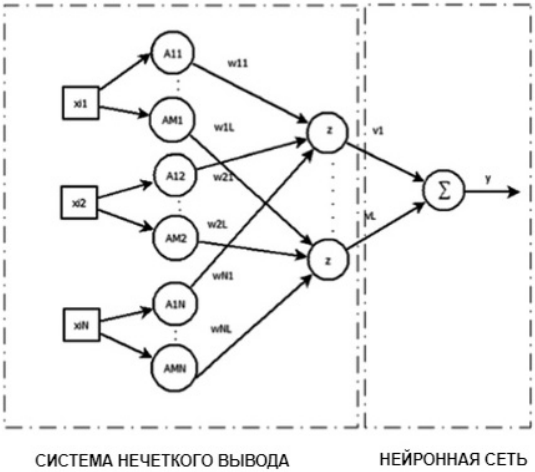

Рис. 1. Архитектура нечеткой нейронной сети

Fig. 1. Fuzzy neural network architecture

Для каждого входного сигнала переменная x_{ij} определяет M как нечеткое множество A^m, где m изменяется от 1 до M, чьи функции принадлежности – это функции активации соответствующих нейронов. Таким образом, атаки с использованием SQL-инъекции являются степенями устойчивости, связанными с входными значениями, то есть $a_j = \mu_m^A$, где j изменяется от 1 до N, m от 1 до M; N – количество входных данных, а M – количество нечетких множеств для каждой входной переменной [10–12]. Для нейронов первого слоя значения смещения и синоптических весов определяются случайным образом в интервале [0, 1].

В настоящей работе мы будем использовать суммарные комбинации нечетких множеств, генерируемых для каждой переменной, когда $N \le 6$. Когда N имеет более высокие числовые значения, мы выполняем случайный выбор

функции принадлежности для каждой входной переменной, где M в этом случае будет в два раза больше значения входного пространства выборок, ограниченного 500 функциями принадлежности. Затем используем SQL-инъекции фаззинейронов модели для определения количества нейронов-кандидатов L_c, представляющих процент от L, где $L_c < L$. По определению, когда $L < 200$, $L_c = 100\ \%L$, в противном случае выбранный коэффициент поможет выбрать нейроны-кандидаты. Этот процент позволяет выбрать наиболее существенные нейроны первого слоя [11].

Второй слой состоит из L_c нечетких нейронов, где выделяется юнинейрон, предложенный в работе [13]. Каждый нейрон выполняет взвешенную сумму некоторых выходов (не всех из-за метода отбора нейронов) первого слоя наряду со смещением и случайно определенными весами юнинейронов [10]. Логические нейроны – это функциональные единицы, которые сочетают логические аспекты обработки с обучаемостью через систему нечетких правил. Их можно рассматривать как многомерные нелинейные преобразования между единичными гиперкубами, $[0,1] \to [0,1]^n$ [10]. Таким образом, нейроны «И» и «ИЛИ» (рис. 2) обновляют значения нечетким вычислением $a = [a_1,\ a_2, ...,\ a_3]$, первоначально комбинируя их по отдельности с их весами $w = [w_1,\ w_2, ...,\ w_3]$ так, что $a,\ w \in [0,1]^n$ для объединения результатов следующим образом [12]:

$$z = or(a,\ w) = S_{i=1}^{N}(a_i s w_i)\ , \tag{1}$$

$$z = and(a,\ w) = T_{i=1}^{N}(a_i t w_i)\ , \tag{2}$$

где T и t – это T-нормы (произведение), а S и s – это S-нормы (вероятностная сумма).

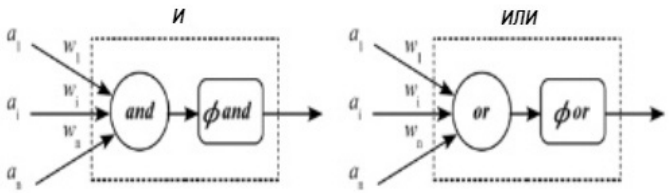

Рис. 2. Схематическое изображение нейронов «И» и «ИЛИ»

Fig. 2. Schematic representation of neurons "AND" and "OR"

U-норма – это обобщение *T*-норм и *S*-норм путем ослабления ограничений, связанных с нейтральными элементами. Вместо значений «0» и «1» для *t*-нормы и *s*-нормы соответственно нейтральному элементу разрешается принимать значения в единичном интервале. Одной из главных характеристик *U*-норм является то, что он больше не имеет так называемого нейтрального элемента, который теперь называется элементом личности [13]. Через этот элемент личности *U*-нормы расширяют *T*-нормы и *S*-нормы с помощью различных значений $g \in [0;1]$, что позволяет чередование *S*-нормы ($g = 0$) и *T*-нормы ($g = 1$) [13]. Формально *U*-норма выражается в виде

$$U(x, y) = \begin{cases} gT\left(\frac{x}{g}, \frac{y}{g}\right), & \text{если } x, y \in [0; g), \\ g + (1-g)S\left(\frac{x-g}{1-g}, \frac{y-g}{1-g}\right), & \text{если } x, y \in (g, 1], \\ \max(x, y) \text{ ИЛИ } \min(x, y), & \text{иначе.} \end{cases} \quad (3)$$

Унинейрон использует понятия *U*-норм для выполнения более упрощенных операций в соответствии с функциями активации нечетких нейронов. Его формализация позволяет унинейрону использовать понятия либо нейрона «И», либо нейрона «ИЛИ». В [13] объясняются важные понятия об унинейроне. Обработка нейронов происходит на двух уровнях. На первом уровне локаций L_1 входные сигналы объединяются индивидуально с весами. Во втором уровне L_2, глобальном, выполняется глобальная операция суммирования по результатам всех комбинаций первого уровня. Традиционные логические нейроны используют *T*-нормы и *S*-нормы для выполнения описанных операций.

Учитывая набор пар $\Omega(a_i, w_i)$, при входном сигнале $a_i \in [0;1]$ и выходном $w_i \in [0;1]$ для выполнения взвешенной агрегации следует выполнить следующие шаги [13]:

1) преобразование каждый пары $\Omega(a_i, w_i)$ в единственное значение:

$$b_i = h(a_i, w_i);$$

2) вычисление единой агрегации преобразованных значений

$$U(b_1,\ b_2,\ldots,\ b_m)\,,$$

где m – это количество входов.

Функция h отвечает за преобразование входных данных и соответствующих весов в индивидуальные преобразованные значения [13]:

$$h(w,\ a) = wa + wg\ . \tag{4}$$

Используя взвешенную агрегацию, можем записать унинейрон следующим образом:

$$z = uni(x,\ w,\ g) = U_{i=1}^{N}(x_i,\ w_i)\,. \tag{5}$$

Нечеткие правила могут быть извлечены через топологию сети в сочетании с унинейрон-логическими нейронами.

После определения нейронов-кандидатов окончательная архитектура сети определяется с помощью выбора подмножества этих нейронов. При выполнении этой процедуры реализуется оптимальное подмножество значений, которое можно рассматривать как задачу выбора переменной, возвращающей наиболее значимые нейроны L_c на основе функции затрат [10]. Аналогично можем интерпретировать этот выбор как выбор наилучшего набора правил, способных представлять входное пространство. Алгоритм обучения предполагает, что атака SQL-инъекции второго слоя нечеткой нейронной сети, состоящей из всех наиболее значимых нейронов L_c, может быть записана в виде

$$f(x_i) = \sum_{i=0}^{L_s} v_i z_i(x_i) = z(x_i)v\,, \tag{6}$$

где $v = [v_0,\ v_1,\ v_2,\ldots,\ v_{L_s}]$ – вектор-столбец весов слоя атаки SQL-инъекции, $z(x_i) = \left[z_0,\ z_1(x_i),\ z_2(x_i),\ldots,\ z_{L_s}(x_i) \right]$ – вектор-строка аргументов второго слоя. В этом контексте $z(x_i)$ рассматривается как нелинейное отображение записи для $(L_s + 1)$-мерных нечетких признаков, выполняемое с использованием выбранных нейронов, поскольку весам, которые связываются с двумя первыми слоями, присваивается случайная форма, а единственными параметрами являются веса SQL-инъекции. Уравнение (6) может быть рассмотрено

как простая линейная регрессионная модель, позволяющая решить задачу выбора наилучших подмножеств нейронов, которые будут идеализированы как модель линейной регрессии для задач выбора [14]. Для выполнения выбора модели был применен широко используемый алгоритм наименьшей угловой регрессии (LARS) [15]. LARS – это регрессионный алгоритм для данных, способный оценить не только коэффициенты регрессии, но и подмножество кандидатов-регрессоров, которые должны быть включены в окончательную модель. Для оценки набора из K различных выборок (x_i, y_i), где $x_i = [x_{i1}, x_{i2}, \ldots, x_{iN}]$, $xx_i, y_i \in \mathbb{R}$, а $i = 1, \ldots, K$, стоимостная функция этого алгоритма регрессии может быть определена как

$$\sum_{i=1}^{K} \left\| z(x_i)v - y_i \right\|_2 + \lambda \left\| v \right\|_1, \tag{7}$$

где λ – параметр регуляризации, оцененный с помощью перекрестной валидации. Первое слагаемое соответствует остаточной сумме квадратов (RSS). Этот терм уменьшается так же, как и ошибка обучения. Второй член –это регуляризационный терм l_1. Формула (7) используется для улучшения обобщения сети без чрезмерной корректировки [14] и может генерировать разреженные модели [15]. Для внесения большей ясности, почему LARS должен использоваться в качестве алгоритма выбора признаков, уравнение следует переписать следующим образом:

$$\min_v RSS(v) st \left\| v \right\|_1 \le \beta, \tag{8}$$

где β – верхняя граница l_1-нормы весов, малое значение β коррелирует с большим значением λ и наоборот. Это уравнение также известно как лассо [15]. Использование лассорегрессии (также называемой l_1-нормой) для нормализации моделей приводит к результатам с пространственными решениями, генерирует результирующие векторы со многими нулями, которые представляют данные, не имеющие значения для анализируемых переменных. Лучший выбор моделей представлен в [14]. Алгоритм LARS может быть использован для выполнения выбора модели, так как при заданном значении λ только некоторые регрессоры имеют равные веса, отличные от нуля. Если $\lambda = 0$, то задача становится неограниченной регрессией с ненулевыми весами.

По мере увеличения $\lambda_{\max}$ от нуля до заданного значения $\lambda_{\max}$ число ненулевых весов уменьшается от N до нуля. Для рассматриваемой в настоя-

щей работе проблемы регрессоры z_{L_s} представляют собой атаки SQL-инъекций значимых нейронов. Таким образом, алгоритм LARS может быть использован для выбора оптимального подмножества жизненно важных нейронов, минимизирующих (8) для заданного значения λ, полученного путем перекрестной валидации. Используя концепцию bootstrap и выполняя пересечение между опорами, Бах [15] разработал модельный корректирующий оценщик без условий консистенции, требуемых для метода лассо. Этой новой процедуре он дал название Bolasso (bootstrap-enhanced least absolute shrinkage operator). Эту структуру можно рассматривать как схему голосования, применяемую для поддержки метода лассо. Однако Bolasso можно рассматривать как режим формирования консенсуса, где поддерживается наиболее значимое подмножество переменных, по которым все регрессоры соглашаются, когда речь идет о выборе переменных [15]. Регрессоры, включаемые в финальную модель, определяются в соответствии с частотой, с которой каждый из них выбирается с помощью различных тестов. Определяется порог консенсуса (например, $\rho = 50\ \%$), и регрессор включается, если он выбран, по крайней мере, в 50 % испытаний. В этой статье загрузчик лассо используется для определения топологии сети и выбора наиболее значимых нейронов. Для вычисления весов атакующего слоя SQL-инъекций применяются концепции экстремальных обучающих машин [15], а нейронная агрегационная сеть, присутствующая в третьем слое модели, выполняет классификацию признаков кибератак в соответствии со следующим уравнением:

$$y = sign\left(f_{\mathrm{Re}\,LU\text{ с утечкой}}\left(\sum_{j=0}^{L_s} z_j v_j \right) \right), \tag{9}$$

где $z_0 = 1$, v_0 – смещение, а z_j, v_j – соответственно величина нечеткого нейрона атаки SQL-инъекции и его вес при $j = 1,..., L_s$; ReLU с утечкой выражается следующей формулой:

$$f_{\mathrm{Re}\,LU\text{ с утечкой}}(z,\ \alpha) = \max(\alpha z,\ z). \tag{10}$$

Эта функция активации в настоящее время используется в задачах различной природы, особенно в тех случаях, когда требуется более высокая чувствительность к результатам, полученным с помощью нечетких нейронных сетей [11–15].

Наконец, после определения топологии сети вычисляется вектор весов слоя атаки SQL-инъекции $v = \left[v_0, v_1, v_2, \ldots, v_{L_s} \right]^T$. В настоящей работе v вычисляется с использованием псевдоинверсии Мура–Пенроуза:

$$v = Z^+ y, \tag{11}$$

где Z^+ – псевдоинверсия Мура–Пенроуза от Z, которая является минимальной нормой решения наименьших квадратов для выходных весов; Z можно определить как

$$Z = \begin{bmatrix} z_0 & z_1(x_1) & \ldots & z_{L_s}(x_1) \\ z_0 & z_1(x_2) & \ldots & z_{L_s}(x_2) \\ . & . & \ldots & . \\ z_0 & z_1(x_n) & \ldots & z_{L_s}(x_n) \end{bmatrix}. \tag{12}$$

Процесс обучения можно резюмировать следующим образом:

1) число нечетких множеств, которые будут разбивать входное пространство, M;

2) процент нейронов-кандидатов, L_c;

3) число повторений начальной загрузки, b;

4) порог консенсуса, ρ.

ЗАКЛЮЧЕНИЕ

Результатом настоящей работы является достаточно полное исследование актуальных на момент написания работы конфигураций, типов и архитектур моделей нечетких нейронных сетей.

Исследование охватывает все базовые типы архитектур нейронных сетей, типов нечетких систем, а также содержит подробную методологию обнаружения атак на базе изученного материала, что позволяет гарантировать применимость данной работы к подавляющему большинству реальных ситуаций.

Исследованы широко используемые во всем мире наборы данных для подготовки и тестирования итоговой нечеткой нейросетевой модели. Подробно описана методология обнаружения атак, а также ее применение относительно атаки, основанной на SQL-инъекции, что способствует облегчению внедрения реализованной системы на реальных объектах.

СПИСОК ЛИТЕРАТУРЫ

1. *McCarthy J.* Programs with Common Sense // Stanford: Computer Science Department. – 1958. – URL: http://jmc.stanford.edu/articles/mcc59/mcc59.pdf (accessed: 14.09.2021).

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. *Першина Э.С., Дараган С.В.* От больших данных к продвинутой аналитике в индустрии туризма // Научный вестник МГИИТ. – 2018. – № 2 (52). – С. 60–69.

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: 10.17212/2782-2230-2021-3-43-56

Methodology for constructing a neural fuzzy network in the field of information security [*]

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 paper proposes the use of hybrid models based on neural networks and fuzzy systems to build intelligent intrusion detection systems based on the theory of fuzzy rules. The presented system will be able to generate rules based on the results using fuzzy logic neurons. To avoid oversaturation and assist in determining the necessary network topology, training models based on extreme learning machine and regularization theory will be used to find the most significant neurons. In this paper, a type of SQL injection cyberattack is considered, which actively exploits errors in systems that communicate with the database via SQL commands, and for this reason is considered a kind of straightforward attack. The fuzzy neural network architecture used in detecting SQL injection attacks is a multi-component structure. The first two layers of the model are considered as a fuzzy inference system capable of extracting

[*] *Received 20 June 2021.*

knowledge from data and transforming it into fuzzy rules. These rules help build automated systems for detecting SQL injection attacks. The third layer consists of a simple neuron that has an activation function called a leaky ReLU. The first layer consists of fuzzy neurons, the activation functions of which are Gaussian membership functions of fuzzy sets, defined in accordance with the partitioning of the input variables. The technique uses the concept of a simple linear regression model to solve the problem of choosing the best subsets of neurons. To perform model selection, the paper used the widely used least angular regression (LARS) algorithm.

Keywords: fuzzy set, fuzzy neural network, information security, neural aggregation network, SQL injection attacks of significant neurons, cyberattack detection model, fuzzy inference system, membership function

REFERENCES

1. McCarthy J. Programs with Common Sense. *Stanford: Computer Science Department*, 1958. Available at: http://jmc.stanford.edu/articles/mcc59/mcc59.pdf (accessed 14.09.2021).

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).

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. Pershina E.S., Daragan S.V. Ot bol'shikh dannykh k prodvinutoi analitike v industrii turizma [From big data to advanced analytics in the tourism industry]. *Nauchnyi vestnik MGIIT = Research Bulletin of MSITI*, 2018, no. 2 (52), pp. 60–69.

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. Методология построения нейронной нечеткой сети в области информационной безопасности // Безопасность цифровых технологий. – 2021. – № 3 (102). – С. 43–56. – DOI: 10.17212/2782-2230-2021-3-43-56.

For citation:

Arkhipova A.B., Polyakov P.A. Metodologiya postroeniya neironnoi nechetkoi seti v oblasti informatsionnoi bezopasnosti [Methodology for constructing a neural fuzzy network in the field of information security]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2021, no. 3 (102), pp. 43–56. DOI: 10.17212/2782-2230-2021-3-43-56.