Научная статья
Original article
УДК 004.032.2

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

FEATURES OF THE USE OF ARTIFICIAL NEURAL NETWORKS IN THE SPHERE OF INFORMATION SECURITY

Арзамасцев Никита Александрович, Студент 2 курс магистратуры, Институт информатики и кибернетики,Самарский национальный исследовательский университет имени академика С. П. Королёва (Самарский университет), Россия, г.Самара

Arzamastsev Nikita Alexandrovich, 2nd year master's student, Institute of Informatics and Cybernetics, Samara National Research University named after Academician S.P. Korolev (Samara University), Russia, Samara

Аннотация: В статье анализируются особенности использования искусственных нейронных сетей в сфере информационной безопасности. Рассматриваются понятие и отличительные характеристики нейронных сетей, приводятся основные разновидности их обучения и возможные процедуры формирования систем обучения. Выявляются понятие успешности, категории и стадии реализации кибератак, определяющие необходимый алгоритм действий. Приводятся возможные характеристики нейронной сети, обеспечивающей информационную безопасность системы.

Annotation: The article analyzes the features of the use of artificial neural networks in the field of information security. The concept and distinctive characteristics of neural networks are considered, the main varieties of their learning and possible procedures for the formation of learning systems are given. The concept of success, categories and stages of implementation of cyberattacks are identified, which determine the necessary algorithm of actions. Possible characteristics of a neural network that ensures the information security of the system are given.

Ключевые слова: информационная система, информационная безопасность, уязвимость, кибератаки, нейронные сети.

Key words: information system, information security, vulnerability, cyber attacks, neural networks.

С увеличением количества предприятий, относимых к критической информационной инфраструктуре, возрастает необходимость обеспечения высокого уровня информационной безопасности их информационных систем [1]. Согласно статистике, число кибератак постепенно увеличивается (в 2021 году их было на 6,7 % больше, чем в 2020), причём 69 % из них имеет целенаправленный характер и ориентировано на сферы здравоохранения и промышленности [2]. При этом существенная часть выявленных уязвимостей информационных систем организаций относится к высокой и критической степеням риска, что ставит под удар сразу три свойства безопасности данных – целостность, конфиденциальность и доступность. Одним из наиболее перспективных направлений своевременного выявления уязвимостей систем информационной безопасности и совершенствования их защиты является использование искусственных нейронных сетей, способных к анализу большого объёма данных [3]. В связи с этим актуальным представляется исследование специфики их применения при решении задач обеспечения информационной безопасности.

Целью работы является изучение особенностей использования искусственных нейронных сетей в сфере информационной безопасности. Для

её достижения были использованы методы анализа и синтеза научных публикаций и литературных источников по рассматриваемой теме.

Нейронная сеть является высокопараллельной динамической системой с топологией направленного графа, могущей получать выходные данные при помощи реакции состояния на входные воздействия [4]. По своей сути нейросети представляют собой формальный аппарат для описания ключевого алгоритма решения прогностических задач в области оценки состояния системы обеспечения информационной безопасности информационных систем по характерным временным сечениям. Их отличительной особенностью является одновременное использование запрограммированных последовательностей работы и наличие способности выявлять закономерности, осуществлять анализ потоковой информации, адаптироваться, обучаться и реализовывать поддержку принятия решений.

Одним их ключевых преимуществ нейронных сетей перед традиционными алгоритмами является возможность обучения, суть которого заключается в определении коэффициентов связей между нейронами [5]. В процессе обучения нейросети способны выявлять сложные зависимости между входными и выходными данными и выполнять их обобщение.

Выделяют три основные разновидности обучения нейронных сетей, включающие ряд возможных процедур формирования системы обучения [6]:

1. Обучение без учителя:

• обучение на основе коррекции ошибок, при котором минимизируется текущее значение величины ошибки на основе дельта-правила Видроу-Хоффа;

• обучение на основе памяти, при котором прошлый опыт нейросети накапливается в базе данных, вследствие чего эффективность обучения зависит от содержательности и объёма примеров и сложности выходного вектора;

• обучение Хебба, опирающееся на правила Хебба, согласно которым если сигнал нейрона неверен и равен нулю, то требуется увеличение веса

входов, на которые была подана единица, а если равен единице, то требуется уменьшение веса этих входов;

- конкурентное обучение, при котором нейроны одного иерархического уровня конкурируют за возможность быть активированными.

2. Обучение с учителем:

- метод наискорейшего спуска, при котором корректировка векторов весов осуществляется в направлении максимального уменьшения функции стоимости, обратном градиенту функции стоимости при значении входных параметров, а в качестве функции стоимости обычно принимается величина отклонения от требуемого выходного значения;
- метод Ньютона, основанный на идее и соотношениях метода Ньютона, касающегося поиска оптимальных решений;
- метод Гаусса-Ньютона, применяющийся для обучения в случае, когда функция стоимости представлена как сумма квадратов отклонений между имеющимся и требуемым выходным набором данных нейросети.

3. Обучение с подкреплением:

- метод обратного распространения ошибок, в процессе которого нейронная сеть обучается при взаимодействии с некой средой, откликом которой на принятые решения выступают сигналы подкрепления.

При помощи нейронной сети возможно не только обеспечить защиту информационной системы от кибератак посредством сетевых систем обнаружения вторжений, но и предотвратить возможность вторжения, своевременно выявив уязвимость [7]. Эффективность таких нейросетей зависит от применяемых методов анализа имеющихся данных о сетевых атаках. Можно выделить следующие категории кибератак [8]:

- Denial of Service Attack (DoS) – отказ в доступе для легального пользователя;
- Remote to Local Attack (R2L) – получение злоумышленником удалённого доступа к системе с неавторизированного устройства;

• User to Root Attack (U2R) – эксплуатация злоумышленником, который получил доступ к системе как рядовой пользователь, уязвимости системы с целью стать «суперпользователем»;

• Probe – сбор данных о вычислительной сети для обхода её системы управления информационной безопасностью.

Успешность кибератаки означает, что методы совершения проникновения оказались новыми и неожиданными для системы информационной безопасности, что и обеспечило возможность проникновения непосредственно в зону обработки данных [9]. Основными особенностями сетевых атак являются высокий уровень непредсказуемости, существенные потери в системе обработки данных и повторяемость атак по попыткам, месту и времени реализации. Атака на активы объекта защиты осуществляется в несколько стадий [10]:

1. Наличие потенциально возможной угрозы, когда объект защиты не может непосредственно влиять на злонамеренное воздействие вследствие нахождения последнего вне контролируемой зоны. Данная ситуация не требует принятия неотложных мер.

2. Атака, в ходе которой угроза проникла в контролируемую зону, но не добралась до зоны хранения представляющих ценность информационных активов. Это предаварийная ситуация, при которой велика вероятность проникновения атаки в зону нахождения данных ограниченного доступа, что требует принятия активных мер, направленных на нейтрализацию атаки.

3. Вторжение, когда атака смогла проникнуть в зону нахождения информационных ценностей и закрытых данных, что требует принятие неотложных мер по её нейтрализации. Эта ситуация является аварийной, поэтому в ней решающим фактором выступает скорость реакции системы обеспечения информационной безопасности.

С учётом специфики кибератак выделяется ряд входных векторов нейронной сети, таких как [11]:

• вектор атаки;

- сложность атаки;
- потребность в привилегиях;
- воздействие с пользователем;
- область действия;
- воздействие на конфиденциальность;
- воздействие на целостность;
- воздействие на доступность.

В качестве выходных данных выступают векторы, соответствующие уровням угроз: низкому, среднему, высокому и критическому. При построении нейросети учитывается набор характеристик, которым обладает каждый пользователь информационной системы, что позволяет определить его типовое поведение [12]. К таким характеристикам могут быть отнесены:

- набор данных, с которыми осуществляется работа;
- место осуществления доступа к системе;
- набор действий, выполняемых пользователем;
- время, в которое осуществляется доступ либо выполняются конкретные действия;
- общая продолжительность действий, которые выполняются в течение определённого времени.

Сама нейронная сеть может иметь различную архитектуру, однако наиболее целесообразным представляется использование многослойных нейросетей обратного распространения ошибки [13].

Таким образом, использование искусственных нейронных сетей в системах информационной безопасности позволяет получать данные о вероятности наличия вторжения в режиме реального времени, что при реальной опасности вторжения даёт возможность своевременно предпринимать меры противодействия. Помимо этого, анализ результатов работы отдельных сетевых подмодулей позволяет получить ответы на ряд важных вопросов касательно обеспечения и совершенствования

информационной безопасности, в частности таких, как выявление потенциально опасных источников вторжения и возможных заражённых источников, сильных и слабых сторон системы обеспечения информационной безопасности, оценка уровня готовности системы к противодействию вторжениям, степень защищённости информационных ценностей и готовность персонала к противодействию вторжениям.

Список литературы

1. Витенбург Е.А. Архитектура программного комплекса интеллектуальной поддержки принятия решений при проектировании системы защиты информационной системы предприятия // Вестник кибернетики. – 2019. – № 4 (36). – С. 46-51.
2. Актуальные киберугрозы: IV квартал 2021 года [Электронный ресурс] // Positive Technologies. – 2022. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q4/ (дата обращения: 08.05.2022).
3. Толстых А.А., Ртищев А.Р., Никитенко В.А. Выбор архитектуры искусственной нейронной сети для обнаружения утечки информации // Пожарная безопасность: проблемы и перспективы. – 2018. – Т. 1, № 9. – С. 887-888.
4. Коцыняк М.А. Управление системой обеспечения безопасности информационно-телекоммуникационной сетью на основе алгоритмов функционирования искусственной нейронной сети / М.А. Коцыняк, М.А. Карпов, О.С. Лаута, В.Е. Дементьев // Известия Тульского государственного университета. Технические науки. – 2020. – № 4. – С. 3-10.
5. Тимочкина Т.В., Татарникова Т.М., Пойманова Е.Д. Применение нейронных сетей для обнаружения сетевых атак // Изв. вузов. Приборостроение. – 2021. – Т. 64, № 5. – С. 357-363.
6. Симаворян С.Ж. Обучение нейронной сети в системах информационной безопасности / С.Ж. Симаворян, А.Р. Симонян, Г.А. Попов, Е.И. Улитина

// Обозрение прикладной и промышленной математики. – 2021. – Т. 28, № 2. – 4 с.

7. Иванов А.Д., Кутищев А.А., Никитина Е.Ю. Разработка приложения для анализа сетевого трафика и обнаружения сетевых атак // Вестник Пермского университета. Математика. Механика. Информатика. – 2021. – № 2 (53). – С. 57-64.
8. Кочетов Д.А., Лукащик Е.П. Нейросетевая технология обнаружения сетевых вторжений // Прикаспийский журнал: управление и высокие технологии. – 2018. – № 2 (42). – С. 104-112.
9. Симаворян С.Ж. Процедура выявления вторжений в системах информационной безопасности на основе использования нейронных сетей / С.Ж. Симаворян, А.Р. Симонян, Г.А. Попов, Е.И. Улитина // Программные системы и вычислительные методы. – 2020. – № 3. – 9 с.
10. Симаворян С.Ж. Общая концепция выявления вторжений неизвестного типа на основе нейронных сетей / С.Ж. Симаворян, А.Р. Симонян, Г.А. Попов, Е.И. Улитина // Программные системы и вычислительные методы. – 2021. – № 4. – С. 23-45.
11. Мельников П.В., Ешенко Р.А. Интеллектуальная система оценки угроз информационной безопасности // Вестник науки. – 2020. – Т. 1, № 6 (27). – С. 179-184.
12. Козин И.С., Рощин А.А. Метод обеспечения безопасности информации при её обработке в информационной системе на основе машинного обучения // Техника средств связи. – 2019. – № 4 (148). – С. 70-82.
13. Жук Р.В., Дзьобан П.И., Власенко А.В. Определение актуальности угроз информационной безопасности в информационных системах обработки персональных данных с использованием математического аппарата нейронных сетей // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 1 (49). – С. 169-178.

Bibliography

1. Vitenburg E.A. Architecture of the software complex for intelligent decision support in the design of the enterprise information system protection system // Bulletin of Cybernetics. - 2019. - No. 4 (36). - S. 46-51.
2. Actual cyber threats: IV quarter of 2021 [Electronic resource] // Positive Technologies. – 2022. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q4/ (date of access: 05/08/2022).
3. Tolstykh A.A., Rtishchev A.R., Nikitenko V.A. The choice of artificial neural network architecture for information leakage detection // Fire safety: problems and prospects. - 2018. - V. 1, No. 9. - S. 887-888.
4. Kotsynyak M.A. Management of the security system of the information and telecommunications network based on algorithms for the functioning of an artificial neural network / M.A. Kotsynyak, M.A. Karpov, O.S. Lauta, V.E. Dementiev // Proceedings of the Tula State University. Technical science. - 2020. - No. 4. - P. 3-10.
5. Timochkina T.V., Tatarnikova T.M., Poimanova E.D. Application of neural networks to detect network attacks // Izv. universities. Instrumentation. - 2021. - T. 64, No. 5. - S. 357-363.
6. Simavoryan S.Zh. Teaching a neural network in information security systems / S.Zh. Simavoryan, A.R. Simonyan, G.A. Popov, E.I. Ulitina // Review of Applied and Industrial Mathematics. - 2021. - T. 28, No. 2. - 4 p.
7. Ivanov A.D., Kutishchev A.A., Nikitina E.Yu. Development of an application for analyzing network traffic and detecting network attacks. Bulletin of the Perm University. Mathematics. Mechanics. Informatics. - 2021. - No. 2 (53). - S. 57-64.
8. Kochetov D.A., Lukashchik E.P. Neural network technology for detecting network intrusions // Caspian journal: management and high technologies. - 2018. - No. 2 (42). - S. 104-112.

9. Simavoryan S.Zh. The procedure for detecting intrusions in information security systems based on the use of neural networks / S.Zh. Simavoryan, A.R. Simonyan, G.A. Popov, E.I. Ulitina // Program systems and computational methods. - 2020. - No. 3. - 9 p.
10. Simavoryan S.Zh. The general concept of detecting intrusions of an unknown type based on neural networks / S.Zh. Simavoryan, A.R. Simonyan, G.A. Popov, E.I. Ulitina // Program systems and computational methods. - 2021. - No. 4. - S. 23-45.
11. Melnikov P.V., Eshenko R.A. Intelligent system for evaluating threats to information security. Vestnik nauki. - 2020. - V. 1, No. 6 (27). - S. 179-184.
12. Kozin I.S., Roshchin A.A. A method for ensuring the security of information during its processing in an information system based on machine learning. - 2019. - No. 4 (148). - S. 70-82.
13. Zhuk R.V., Dzioban P.I., Vlasenko A.V. Determining the relevance of information security threats in information systems for processing personal data using the mathematical apparatus of neural networks // Caspian Journal: Management and High Technologies. - 2020. - No. 1 (49). – S. 169-178.

© *Арзамасцев Н.А., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №5/2022.*

Для цитирования: Арзамасцев Н.А. ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №5/2022.