ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 28 МАТЕМАТИКИ Выпуск 2
2021

С. Ж. Симаворян, **А. Р. Симонян**, **Е. И. Улитина**, **Г. А. Попов** (Сочи, СГУ, Астрахань, АГТУ)**. Обучение нейронной сети в системах информационной безопасности.**

УДК 004.02

Резюме: Вопрос об организации системы обучения нейронной сети является одним из ключевых в области информационной безопасности. В рамках рассматриваемой задачи необходимо провести анализ существующих парадигм обучения нейронных сетей и предложить новую эффективную схему обучения применительно к системам обнаружения вторжений в системах информационной безопасности.

Ключевые слова: нейронная сеть, информационная безопасность, обучение нейронной сети, система обнаружения вторжений.

Применительно к нейронной сети (НС) обучение — это процесс, в котором свободные параметры НС настраиваются посредством моделирования среды, в которую эта сеть встроена. Тип обучения определяется способом подстройки этих параметров, например, в НС поступают стимулы из внешней среды, в результате этого изменяются свободные параметры НС, после изменения внутренней структуры НС отвечает на возбуждения уже иным образом. Свободными параметрами НС являются, прежде всего, вероятности всех переходов из нейронов более высшего уровня иерархии к следующему уровню. Существуют три основные парадигмы обучения НС: 1) обучение без учителя; 2) обучение с учителем; 3) обучение с подкреплением. Наиболее простыми, но наименее адаптивными являются методы обучения без учителя. Многие из них опираются на классические методы оптимизации поиска. Ниже приведены наиболее известные из указанных методов. В рамках перечисленных парадигм обучения имеется достаточно представительный ряд возможных процедур формирования системы обучения. Кратко перечислим основные из них (см. [1], [2], [3]).

1. Обучение без учителя: а) обучение, основанное на коррекции ошибок — минимизируется текущее значение величины ошибки, минимизация функции ошибки выполняется на основе дельта-правила Видроу-Хоффа; б) обучение на основе памяти — при данном виде обучения весь прошлый опыт накапливается в базе данных, эффективность обучения существенно зависит от объема и содержательности примеров и несложности выходного вектора; в) обучение Хебба — метод опирается на следующее два правила Хебба: 1) если сигнал нейрона неверен (его необходимо изменить) и равен нулю, то необходимо увеличить веса тех входов, на которые была подана единица; 2) если сигнал неверен и равен единице, то необходимо уменьшить веса тех входов, на которые была подана единица; г) конкурентное обучение - в конкурентном обучении нейроны одного уровня иерархии сражаются за право быть активированными.

2. Обучение с учителем: а) метод наискорейшего спуска — в данном методе, по аналогии с методами градиентного спуска, корректирока векторов весов выполняется в направлении максимального уменьшения функции стоимости, в направлении, обратном градиенту функции стоимости при данном значении входных параметров, в качестве функции стоимости обычно берется величина отклонения (ошибки) от желаемого

или требуемого выходного значения; б) метод Ньютона — используются идеи и соотношения метода Ньютона поиска оптимальных решений (имеющего сверх потенциальную скорость сходимости); в) метод Гаусса-Ньютона — данный метод применяется для обучения в важном частном случае, когда функция стоимости представлена в виде суммы квадратов отклонений (ошибок) между имеющимся и желаемым выходным набором НС.

3. Обучение с подкреплением: метод обратного распространения ошибок — это один из способов машинного обучения, в ходе которого НС обучается, взаимодействуя с некоторой средой; откликом среды (а не специальной системы управления подкреплением, как это происходит в обучении с учителем) на принятые решения являются сигналы подкрепления, поэтому такое обучение является частным случаем обучения с учителем, но учителем является среда или её модель. Встает задача выбрать наиболее приемлемую из них применительно к НС по выявлению вторжений на базе системного подхода (см [4], [5]). Применительно к системам обнаружения вторжений (СОВ) предлагается использовать концепцию обучения с учителем (ОсУ) по следующим причинам:

1. Процедура ОсУ позволяют субъекту-учителю (понимаемому в обобщенным смысле как некая среда, включающая потенциально много отдельных субъектов) принимать активное участие в процессе обучения. В системах информационной безопасности (ИБ) это важно, поскольку позволяет учитывать индивидуальные особенности объекта защиты и самой системы ИБ.

2. Обучение без учителя опирается обычно на статистический, экспериментальные и/или иные реальные данные, на основе которых строится обучающая выборка. Однако, в сфере ИБ подобных данных часто крайне мало и недостаточно для полноценного обучения НС. Процедура ОсУ позволяет активно и адаптивно использовать обучающие выборки, формируемые искусственно с привлечением экспертов и различных экспертных данных.

3. НС, обученные на основе процедуры ОсУ, позволяют более оперативно, более точно и более адаптивно использовать различные процедуры уточнения и модификации данных с учетом таких факторов как устаревание имеющихся данных, адаптация данных к текущим особенностям объекта защиты и системы ИБ, корректировка данных с учетом недостаточной согласованности мнений экспертов.

4. Вектор, описывающий состояние среды функционирования системы, в системе ИБ может быть неполным, отдельные данные могут иметь большую погрешность, быть приближенными. В этих ситуациях компетентный эксперт-учитель, опираясь на свои и сторонние знания и опыт, может выполнять корректировку этих данных. Все методы обучения без учителя не позволяют в приведенной выше их реализации активно участвовать эксперту с целью адаптации имеющихся примеров обучения, что, как следует из предыдущего анализа, не позволяет эффективно обучать НС по вторжениям. В случае обучения с подкреплением в качестве учителя выступает некая несубъектная сущность (модель, среда), то есть участие эксперта с возможностью эффективной адаптации данных к реальным объектам крайне ограничено или даже невозможно. На рис. приведена разработанная общая схема обучения с учителем применительно к системам ИБ. Напомним, в системах ОсУ основной целью является подбор таких значений внутренних параметров НС, которые бы обеспечили принятие сетью решений, наиболее близких к мнению эксперта или к реальному результату, известному для данного набора входных параметров. Степень близости обычно оценивается величиной квадратичного отклонения между оценкой, полученной с помощью НС, и желаемой или известной оценкой. Одной из особенностей разработанной схемы является опосредованное использование базы (БД) данных по инцидентам, когда каждый пример из БД непосредственно для обучения не используется, а предварительно анализируется учителем. Это связано с необходимостью учета всех особенностей объекта и системы защиты, а также быстрым устареванием данных, так как в процессах информацион-

ного противоборства и противостояния анализ ситуации и ошибок, корректировка и реализация новых атак обычно осуществляются достаточно оперативно. При этом учитель, на основе анализа входных данных, может также формировать свои варианты обучающих выборок.

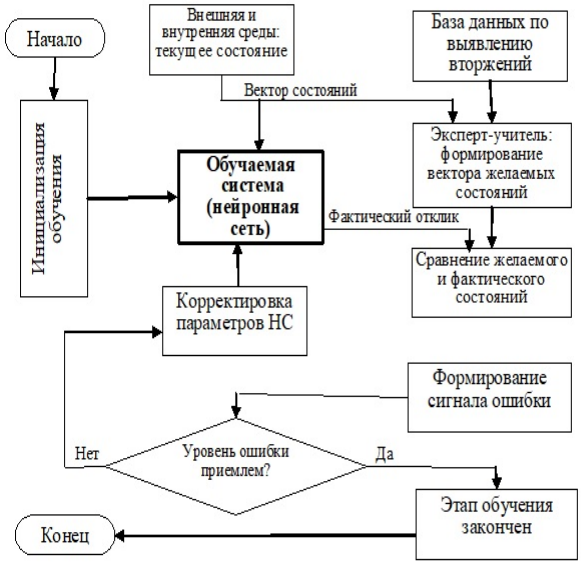

Рис. Общая схема обучения с учителем в системах выявления и противодействия вторжениям

Укажем также на большую значимость по сравнению с другими сферами этапа инициализации обучения: чем точнее, ближе к реальному выбрано начальное состояние, тем меньше итераций потребуется для достижения результата — в системах информационной безопасности обычно примеров много не бывает.

Благодарности. Работа выполнена при финансовой поддержке гранта РФФИ № 19-01-00383.

СПИСОК ЛИТЕРАТУРЫ

1. *Ростовцев В. С.* Искусственные нейронные сети: учебник. Санкт-Петербург, Лань, 2019, 216 с.
2. *Аггарвал Ч.* Нейронные сети и глубокое обучение. СПб, ООО «Диалектика», 2020, 752 с.
3. *Рашид Т.* Создаем нейронную сеть. СПб: ООО «Альфа-книга», 2018, 272 с.
4. *Симаворян С. Ж.*, *Симонян А. Р.*, *Улитина Е. И.*, *Попов Г. А.* О концепции создания интеллектуальных систем защиты информации на основе нейросетевых систем обнаружения вторжений в АСОД. — Программные системы и вычислительные методы, 2019, № 3, с. 30–36.
5. *Симаворян С. Ж.*, *Симонян А. Р.*, *Попов Г. А.*, *Улитина Е. И.* Процедура выявления вторжений в системах информационной безопасности на основе использования нейронных сетей. — Программные системы и вычислительные методы, 2020, № 3, с. 1–9.

UDC 004.02

Simavoryan S. Zh., Simonyan A. R., Ulitina E. I., Popov G. A. (Sochi, Sochi State University, Astrakhan, Astrakhan State Technical University)**.. Neural network training in information security systems.**

Abstract: The issue of organizing a neural network training system is one of the key issues in the field of information security. Within the framework of this task, it is necessary to analyze the existing training paradigms of neural networks and propose a new effective training scheme for intrusion detection systems in information security systems.

Keywords: neural network, information security, neural network training, intrusion detection system.