ЭФФЕКТИВНОЕ ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАЩИТЕ ОТ КИБЕРАТАК

Авторы: *Шапошников Олег Викторович (Иркутский Национальный Исследовательский Технический Университет)*

Аннотация: *Актуальность и постановка задачи: возрастающая роль информации в современном обществе неизмеримо возросла, и актуальность использования современных методов защиты дает возможность своевременного выполнения своей функции. В работе автор использует технологии искусственного интеллекта для идентификации кибератак.*

Ключевые слова: *искусственный интеллект, нейронная сеть, кибератака, оценка эффективности атак злоумышленника, нейросетевое моделирование.*

1 Введение

В современном мире системы защиты информации от кибератак представляют собой одно из главных средств защиты ресурсов компьютерных сетей и систем. Применение подобных систем осуществляется давно, над созданием подобных средств трудятся опытные специалисты, но и научно-методической базе уделено множество работ, вместе с тем практический опыт дает понять, что в системах защиты от сетевых кибератак имеется ряд важных недостатков. Низкая точность идентификации общей совокупности атак – является одним из них, что в свою очередь доказывается определенными событиями взлома систем защиты в ряде ведущих стран [1]. Применение структуры искусственных нейронных сетей является перспективным способом повышения продуктивности систем предотвращения атак, на что также указывают научные труды высококвалифицированных специалистов [3; 4].

Таким образом, задача разработки эффективной технологии искусственного интеллекта идентификации кибератак и последствий инцидентов в реальном времени обуславливает актуальность научных исследований и разработок в данной области.

2 Постановка задачи

Основная задача – разработка технологии искусственного интеллекта идентификации кибератак. Для построения технологии требуется провести анализ возможностей средств нейронных сетей в области предотвращения атак в кибернетическом пространстве.

3 Исследовательский вопрос предотвращения кибератак на информационные системы

На начальном этапе мероприятия по защите информационных систем сводятся к регистрации успешных случаев кибератак на ресурсы таких систем в отношении их уязвимостей. В выпускной квалификационной работе особое внимание уделяется обнаружению и классификации кибератак,

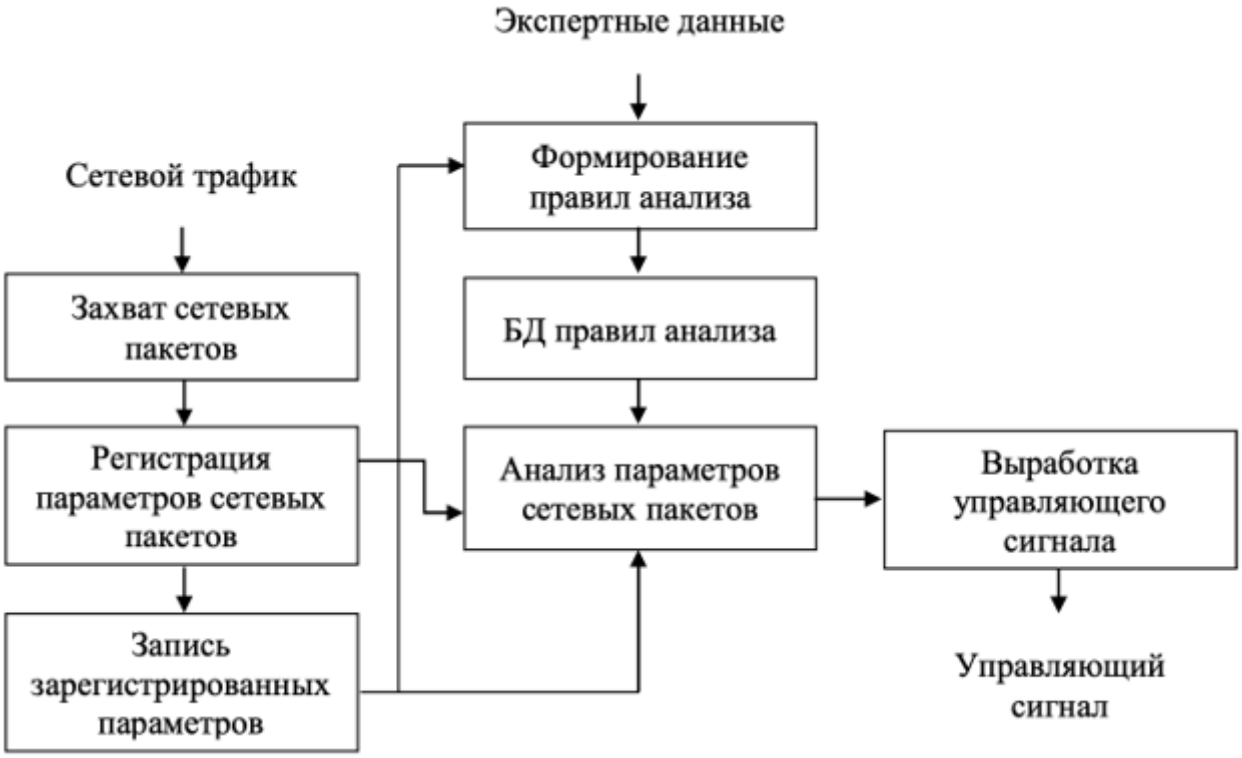

Рисунок 1. Работа системы предотвращения атак

осуществляемых с использованием сетевого трафика. Так как выводы [6; 7; 8; 9] говорят о том, что на сегодняшний день данный тип атак представляет собой один из наиболее опасных. Как правило для регистрации событий сетевых кибератак применяются системы предотвращения атакам, которые являются совокупностью средств, направленных для мониторинга событий в системе и их анализа на предмет признаков нарушения безопасности данной системы. Порядок работы системы предотвращения атак представлен на рисунке 1.

Основываясь на результатах таких работ как [12; 13], можно сделать вывод о том, что усовершенствование систем предотвращения атак заключается в улучшении эффективности анализа трафика.

4 Изучение процесса предотвращения атак

Процесс предотвращения атак на сегодняшний день осуществляется с применением двух подходов: нахождения отклонений и распознавания злоупотреблений.

Работа системы при нахождении отклонений основывается на анализе, что индикатором атаки является отклонение действующих значений трафика от значений, присущих нормальному состоянию ресурсов информационной системы. В свою очередь системы предотвращения атак применяющие метод распознавания злоупотреблений, подвергают анализу серию событий, относящихся к работе предмета защиты и сопоставляют их с типовыми экземплярами известных атак. Данные экземпляры, как правило, называются образцом атак, а метод носит название – распознавание атак на основе сигнатур. Эти подходы имеют как преимущества, так и принципиальные недостатки.

5 Способы совершенствования средств предотвращения атак

Итогом осуществленного анализа показано, что улучшение нейросетевого обнаружения атак осуществляется при помощи реализации некоторых функций, которые трактуются параметрами, отраженными в таблице 1.

Выполнен вывод, что повышение продуктивности нейросетевых средств в большей мере зависит от общей полноты и респектабельности обучающей выборки.

Помимо этих функций имеется зависимость, принимается ли во внимание при кодировании выходного сигнала сходство образцов, определяемых классов атак. Настоящий вывод изложен на праве анализа итогов научного труда [16]. На основе этого, предлагается применение E(ов) и E(квс) параметров, представление которых отражено в таблице 1.

Со временем номенклатура данных параметров имеет возможность к увеличению.

Таблица 1.

Параметры анализа продуктивности нейросетевых методов

Название параметра	Описание
$E_{пп}$	Предварительная подготовка входящих величин
$E_{ппа}$	Повышение эффективности архитектуры
$E_{пва}$	Повышение эффективности величин архитектуры
$E_{пэо}$	Повышение эффективности способа обучения
$E_{соп}$	Способность обучения посредством экспертных правил
$E_{сис}$	Способность использования в методе многообещающих видов нейронный структур
$E_{сор}$	Способность концептуальной оценки рациональности использования нейросетей для выполнения задачи
$E_{оов}$	Присутствие процесса организации обучающей выборки из различных данных
$E_{ппк}$	Присутствие процесса кодирования необходимого выходного признака, учитывающего схожесть образцов рассматриваемых типов атак

Показатели представленных параметров допускается рассмотреть по бинарной классификации: 0 и 1. Величина равняется 0, если способ не осуществим и 1 в ином случае. Для рассмотренных примеров показатели представленных параметров отражены в таблице 2. Также для всех рассмотренных методов $E_{ппк} = 0$. Это значит, что во множестве из рассмотренных методов не реализована операция создания обучающей выборки. Применение рекомендованных параметров способствует определению уровня эффективности нейросети.

Таблица 2.

Параметры определяющие производительность методов работы нейросети

Метод	Параметр								
	$E_{пп}$	$E_{ппа}$	$E_{пва}$	$E_{пэо}$	$E_{соп}$	$E_{сис}$	$E_{сор}$	$E_{оов}$	$E_{ппк}$
№1	1	0	0	0	0	0	0	0	0
№2	0	1	0	0	0	0	0	0	0

№3	1	1	0	0	0	0	0	0	0
№4	0	1	1	0	0	0	0	0	0
№5	0	1	1	0	0	0	0	0	0
№6	1	0	0	0	0	0	0	0	0
№7	1	1	0	1	0	0	0	0	0
№8	1	1	1	0	0	0	0	0	0
№9	0	1	0	1	0	0	0	0	0
№10	0	1	0	1	0	0	0	1	0
№11	1	0	0	0	0	0	0	1	0
№12	1	0	0	0	0	0	0	0	0
№13	1	0	0	0	0	0	0	0	0
№14	1	0	0	0	0	0	0	1	0
№15	1	0	0	0	0	0	0	1	0
№16	1	1	1	1	1	1	1	0	0
№17	1	0	1	0	0	0	0	0	0
№18	1	1	1	1	0	0	0	0	0
№19	1	0	0	1	0	0	0	0	0
№20	1	0	1	1	0	0	0	0	0
№21	1	0	1	1	0	1	0	0	0

Ценность таблицы заключается в отражении минусов и плюсов возможностей повышения эффективности существующих моделей и систем.

К примеру, параметр $E_{ппа} = 0$ говорит о том, что к минусу данного метода позволено отнести низкую оптимизацию типа структуры нейросети. Вместе с тем, в итоге осуществленного исследования показано, что в большей мере применяются традиционные виды нейросетей – это допускает сжать круг возможных типов нейросетей. Что позволяет улучшить эффективность установления модели, наиболее подходящей в аспекте определенной задачи.

7 Выводы по исследованию:

Итогом оценки научных трудов посвященных созданию и использованию систем

определения атак в киберпространстве показано, что среди множества способов улучшения данных систем одним из основных является введение в них метода анализа трафика сетевого типа, основывающегося на актуальных решениях концепций искусственного интеллекта. Настоящей задачей также является внедрение аспекта искусственного интеллекта в сетевые механизмы распознавания атак.

Вместе с тем, анализ подходов к определению атак дал постановить, что повышение их результативности в большинстве случаев опирается на приспособление к ожидаемой картине использования, которая в свою очередь зависит от условий создания примеров обучающей выборки. В конечном итоге появляется необходимость повышения качества методологической базы рассматриваемой темы и созданию на этой базе метода разработки обучающей выборки и метода разработки равнозначных нейросетевых моделей. Для апробации представленных идей рационально спроектировать нейросетевую модель и произвести испытание ее эффективности.

Список литературы:

1. Абрамов Е.С. Разработка и исследование методов построения систем обнаружения атак: дис. ... канд. техн. наук: 05.13.19. − Таганрог, 2005. − 199 с.
2. Васильев В.И., Хафизов А.Ф. Нейронные сети при обнаружении атак в сети Internet (на примере атаки SYNFLOOD) // Нейрокомпьютеры в информационных и экспертных системах. – М.: Радиотехника, 2007. – №6. – С. 34-38.
3. Гришин А.В. Нейросетевые технологии в задачах обнаружения компьютерных атак // Информационные технологии и вычислительные системы. – 2011. – №1. – С. 53 -64.
4. Емельянова Ю.Г., Талалаев А.А., Тищенко И.П. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы // Программные системы: теория и приложения. – 2011. – №3(7). – С. 3–15.
5. Большев А.К. Алгоритмы преобразования и классификации трафика для обнаружения вторжений в компьютерные сети: авторефер. ... канд. техн. наук: 05.13.19 – Методы и системы защиты информации, информационная безопасность. − Санкт-Петербург, 2011. − 36 с.
6. Комар М.П. Метод построения совокупного классификатора трафика информационно-телекоммуникационных сетей для иерархической классификации компьютерных атак // Системи обробки інформації. – 2012. – Випуск 3 (101) . – Том 1 – С.134-138.
7. Аль-Мехди С.Т., Евланенкова О. Применение нейронных сетей для обнаружения вторжений // Доклады ТУСУР. – 2014. – №4. – С. 28-33.
8. Магницкий Ю.Н. Использование бинарной нейронной сети для обнаружения атак на ресурсы распределенных информационных систем // Динамика неоднородных систем. − 2008. − С. 200-205.
9. Planquart J.P. Application of neural networks to intrusion detection [Electronic resource] // SANS Information Security Reading Room. – Electronic data. – [USA]: SANS Institute, 2001. – URL: http://www.sans.org/reading_room/ whitepapers/detection/application-neural-

networks-intrusion-detection_336. – Language: English. – Description based on home page (viewed on 16.04.22).
10. Крыжановский А.В. Применениеискусственныхнейронныхсетей всистемахобнаруженияатак [Электронный ресурс] // ДокладыТУСУРа. – 2008. – No 2 (18). – Часть – С. 37-41. https://cyber leninka.ru/article/n/primenenie-iskusstvennyh-neyronnyh-setey-v-sistemah-obnaruzheniya-atak. 19.04.2022.
11. Слеповичев И.И., Ирматов П.В., Комарова М.С., Бежин А.А. Обнаружение DDoS-атак нечеткой нейронной сетью // Известия Саратовского университета. Серия «Математика. Механика. Информатика». – 2009. – Т. 9. – Вып. 3. – С. 84-89.
12. Комар М.П., Палий И.О., Шевчук Р.П. Нейросетевой подход к обнаружению сетевых атак на компьютерные системы // Інформатика та математичні методи в моделюванні. – 2011. – Том 1. – №2. – С. 156-160.
13. Корченко А.Г., Терейковский И.А., Карпинский Н., Тынымбаев С. Нейросетевые модели, методы и средства оценки параметров безопасности интернет-ориентированных информационных систем: монография. - К.: ТОО «Наш Формат». – 2016. – 275 с.
14. Міхайленко В.М., Терейковська Л.О., Терейковський І.А., Ахметов Б.Б. Нейромережеві моделі та методи розпізнавання фонем в голосовому сигналі в системі дистанційного навчання: монографія. – К.: ЦП «Компринтр», 2017. – 252 с.
15. Bivens A., Palagiri C., Smith R., Szymansky B. Network – Based Intrusion Detection Using Neural Networks // Proc. Intelligent Engineering Systems through Artificial Neural Networks ANNIE. – 2002. – St. Louis, MO. – Volume 12. – New York: ASME Press, 2002. – P. 579-584.
16. Kang M., Kang J. Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security // PLoS One 2016; 11(6).
17. Hnatiuk S. Cyberterrorism: History of current trends and countermeasures // Privacy Notice. – 2013. – Volume 9. – №2. – P. 118-129.