DOI 10.37882/2223–2966.2022.04.29

ВЫБОР ОПТИМАЛЬНОГО АЛГОРИТМА ВЫЯВЛЕНИЯ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАЗЕМНОГО КОМПЛЕКСА УПРАВЛЕНИЯ ПОЛЕТАМИ ДЛЯ СПУТНИКОВОЙ СЕТИ СВЯЗИ

Савельев Роман Николаевич
Аспирант, Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, г. Красноярск
savelyevroman@mail.ru

Аннотация. Представлена разработка блок-схемы предлагаемой процедуры контроля защищенности информационной системы наземного комплекса управления полетами для спутниковой сети связи. Установлено, что использование нейронных сетей является эффективным при выявлении нарушений информационной безопасности наземного комплекса управления полетами. Представлены основные алгоритмы нейронных сетей, которые могут быть использованы для выявления нарушений информационной безопасности. Показаны возможности использования нейронных сетей для контроля защищенности информационной системы наземного комплекса управления полетами. Установлено, что ИНС лучше распознают шаблоны и выявляют нарушения, даже если они не следуют установленным векторам атаки, а ИНС могут автоматически решать многие проблемы без какого-либо вмешательства человека. Это означает, что наземный комплекс управления полетами будет тратить меньше времени на поиск ложных срабатываний и устранение незначительных угроз. Инструменты анализа поведения пользователей и сущностей расширяют технологию за счет использования нейронных сетей для мониторинга учетных записей пользователей, а также компьютеров, таких как конечные точки, маршрутизаторы и серверы. Представлена математическая модель обучения нейронной сети для выявления нарушений информационной безопасности. Представленное позволяет установить, что использование нейронных сетей для наземного комплекса управления полетами использовать целесообразно. Цель работы: разработка алгоритма выявления нарушений информационной безопасности наземного комплекса управления полетами для спутниковой сети связи с помощью использования нейронных сетей. При написании статьи были использованы методы анализа, сравнения, обобщения, математического моделирования. В результате выполнения работы разработан алгоритм выявления нарушений информационной безопасности и показана целесообразность применения машинного обучения. Представленные результаты могут быть использованы наземными комплексами управления спутниковой сети для повышения информационной безопасности и выявления нарушений и возможных атак.

Ключевые слова: информационная безопасность, спутниковая сеть, нейронная сеть, алгоритм обучения, эффективность.

SELECTION OF THE OPTIMAL ALGORITHM FOR DETECTING INFORMATION SECURITY BREACHES OF THE GROUND FLIGHT CONTROL COMPLEX FOR A SATELLITE COMMUNICATION NETWORK

R. Saveliev

Summary. The development of a block diagram of the proposed procedure for monitoring the security of the information system of a ground-based flight control complex for a satellite communication network is presented. It has been established that the use of neural networks is effective in detecting violations of the information security of the ground-based flight control complex. The main algorithms of neural networks that can be used to detect violations of information security are presented. The possibilities of using neural networks to control the security of the information system of the ground-based flight control complex are shown. It has been found that ANNs are better at recognizing patterns and detecting violations even if they do not follow established attack vectors, and ANNs can automatically solve many problems without any human intervention. This means that ground mission control will spend less time looking for false positives and eliminating minor threats. User and entity behavior analysis tools extend the technology by using neural networks to monitor user accounts as well as computers such as endpoints, routers, and servers. A mathematical model for training a neural network to detect information security violations is presented. The presented allows us to establish that it is advisable to use neural networks for the ground-based flight control complex. Purpose of the work: development of an algorithm for detecting violations of information security of the ground-based flight control complex for a satellite communication network using neural networks. When writing the article, methods of analysis, comparison, generalization, and mathematical modeling were used. As a result of the work, an algorithm for detecting information security violations was developed and the expediency of using machine learning was shown. The presented results can be used by ground-based satellite network control systems to improve information security and detect violations and possible attacks.

Keywords: information security, satellite network, ground complex, monitoring, cryptographic protection.

Введение

Деятельность наземного комплекса управления полетами напрямую зависит от эффективности обработки информации в многоуровневых информационных системах, таких как персональные компьютеры, облачные хранилища, корпоративные сети и т.д. Одним из главных условий успешного функционирования является обеспечение защиты информации, которая циркулирует в рамках инфокоммуникационной среды и является критически важной [1].

Наличие телекоммуникационной сети позволяет пользователям совместно использовать программы и данные, что увеличивает угрозу безопасности. Используя распределенные сети, можно столкнуться с различными угрозами: перехватом информации (раскрытием), ее искажением, подменой, блокировкой и другое. Поэтому важно проектировать инфокоммуникационною среду с соблюдением всех современных требований информационной безопасности, в том числе и для наземного комплекса управления полетами [2].

Постановка задачи

В настоящее время начинают широко использоваться нейронные сети во многих сферах жизнедеятельности, в том числе и в средствах защиты информации. Именно поэтому повышение информационной безопасности наземного комплекса управления полетами с использованием нейронных сетей является актуальным направлением исследований [3].

Целью написания статьи является разработка алгоритма выявления нарушений информационной безопасности наземного комплекса управления полетами для спутниковой сети.

Основная часть

Искусственные нейронные сети (ИНС) — это статистические модели, предназначенные для адаптации и самопрограммирования с использованием обучающих алгоритмов. Входной слой аналогичен дендритам в нейронной сети человеческого мозга.

Скрытый слой сравним с телом клетки и находится между входным слоем и выходным слоем (который является родственным синаптическими выходами в головном мозге).

Скрытый слой — это место, где искусственные нейроны принимают набор входных данных на основе синаптического веса, который представляет собой амплитуду или силу связи между узлами. Эти взвешенные входные данные генерируют выход через передаточную функцию на выходной слой [4–6].

Рассмотрим в табличной форме основные алгоритмы обучения нейронных сетей (таблица 1) [7–9].

В настоящее время нейронные сети в области информационной безопасности используются несколькими способами с целью повышения безопасности данных. Ниже представлено несколько примеров технологий защиты данных, которые расширяются за счет нейронных сетей [10,11].

1. Системы обнаружения и предотвращения вторжений (IDS / IPS). Традиционно системы обнаружения и предотвращения вторжений использовали алгоритмы машинного обучения или обнаружение на основе сигнатур для отслеживания сетевой активности и предотвращения вторжений.

2. Аналитика поведения пользователей и объектов

Помимо обнаружения нарушений, также можно использовать ИНС для мониторинга и анализа поведения авторизованных пользователей в ИС сети.

Подобные решения изучают базовые параметры нормальной активности в сети, поэтому они могут легко обнаруживать аномальные или подозрительные действия, такие как необычное время входа в систему или большие объемы передачи данных.

3. Антивредоносное ПО. Традиционные антивирусные и антивредоносные решения работают для предотвращения вирусов и других видов вредоносного программного обеспечения (также известного как вредоносное ПО) путем сравнения файлов с базой данных известных угроз, чтобы определить, опасны они или нет.

Все вышеперечисленное показывает о возможности использования ИНС в системах обеспечения информационной безопасности с целью повышения ИБ и контроля защищенности информационной системы [12,13].

Основными компонентами систем мониторинга информационной безопасности являются: программные агенты, сервер, хранилища информации, консоль, персонал, регламенты работы по мониторингу [14].

Любая система мониторинга событий информационной безопасности может быть отнесена к одной из следующих категорий:

1. SIEM (Security Information and Event Management) — системы, которые отслеживают

Таблица 1. Основные алгоритмы нейронных сетей

Алгоритм	Цель
Автоэнкодер (AE)	Обычно AE используется для уменьшения количества рассматриваемых случайных величин, чтобы система могла изучить представление для набора данных и, следовательно, обработать генеративные модели данных.
Двунаправленная рекуррентная нейронная сеть (BRNN)	Цель BRNN — увеличить информационные входы, доступные для сети, путем подключения двух скрытых, направленных противоположных слоев к одному и тому же выходу. Используя BRNN, выходной слой может получать информацию как из прошлого, так и из будущего состояния.
Машина Больцмана (BM)	Рекуррентная нейронная сеть, этот алгоритм способен изучать внутренние представления и может представлять и решать сложные комбинированные задачи.
Сверточная нейронная сеть (CNN)	CNN, наиболее часто используемые для анализа визуальных образов, представляют собой нейронную сеть с прямой связью, предназначенную для минимизации предварительной обработки.
Глубокая остаточная сеть (DRN)	DRN помогают в решении сложных задач и моделей глубокого обучения. Имея много уровней, DRN предотвращает ухудшение результатов.
Автоэнкодер с шумоподавлением (DAE)	DAE используется для восстановления данных из поврежденных входных данных; алгоритм заставляет скрытый слой изучать более надежные функции. В результате на выходе получается более точная версия входных данных.
Сеть состояния эха (ESN)	ESN работает со случайной большой фиксированной рекуррентной нейронной сетью, в которой каждый узел получает нелинейный ответный сигнал. Алгоритм случайным образом устанавливает и назначает веса и возможности подключения для достижения гибкости обучения.
Нейронная сеть прямого распространения (FF или FFNN) и персептрон (P)	Это базовые алгоритмы нейронных сетей. Нейронная сеть прямого распространения — это искусственная нейронная сеть, в которой соединения узлов не образуют цикл; перцептрон — это бинарная функция, имеющая только два результата (вверх / вниз; да / нет, 0/1).
Генеративная состязательная сеть (GAN)	Эта система противопоставляет две нейронные сети — дискриминационную и генеративную. Цель состоит в том, чтобы различать реальные и синтетические результаты для моделирования концептуальных задач высокого уровня.
Сеть Хопфилда (HN)	Эта форма рекуррентной искусственной нейронной сети представляет собой систему ассоциативной памяти с бинарными пороговыми узлами. Созданные для сведения к локальному минимуму, HN представляют собой модель для понимания человеческой памяти.
Сеть Кохонена (KN)	KN организует проблемное пространство в двумерную карту. Разница между самоорганизующимися картами (SOM) и другими подходами к решению проблем заключается в том, что SOM используют конкурентное обучение, а не обучение с исправлением ошибок.
Цепь Маркова (MC)	MC — это математический процесс, который описывает последовательность возможных событий, в которой вероятность каждого события зависит исключительно от состояния, достигнутого в предыдущем событии
Сети радиальных базисных функций (сети RBF)	Разработчики используют сети RBF для моделирования данных, которые представляют основную тенденцию или функцию. Сети RBF учатся аппроксимировать основной тренд, используя кривые колокола или нелинейные классификаторы. Нелинейные классификаторы анализируют более глубоко, чем простые линейные классификаторы, которые работают с векторами меньшей размерности.
Рекуррентная нейронная сеть (RNN)	PHC моделируют последовательные взаимодействия через память. На каждом временном шаге RNN вычисляет новую память или скрытое состояние в зависимости от текущего входного и предыдущего состояния памяти.
Ограниченная машина Больцмана (RBM)	RBM — это вероятностная графическая модель в неконтролируемой среде. RBM состоит из видимых и скрытых слоев, а также связей между бинарными нейронами в каждом из этих слоев. RBN полезны для фильтрации, изучения функций и классификации.
Машина опорных векторов (SVM)	На основе наборов обучающих примеров, относящихся к одной из двух возможных категорий, алгоритм SVM строит модель, которая относит новые примеры к одной из двух категорий. Затем модель представляет примеры в виде нанесенных на карту точек в пространстве, при этом эти примеры отдельных категорий делятся на максимально возможный промежуток. Затем алгоритм отображает новые примеры в том же пространстве и предсказывает, к какой категории они относятся, в зависимости от того, на какой стороне разрыва они занимают.
Вариационный автоэнкодер (VAE)	VAE — это особый тип нейронной сети, которая помогает создавать сложные модели на основе наборов данных. В общем, автоэнкодер — это сеть глубокого обучения, которая пытается восстановить модель или сопоставить целевые выходные данные с предоставленными входными данными посредством обратного распространения.

и анализируют события в режиме реального времени.
2. UBA (User Behavioral Analytics) — системы, которые собирают данные о действиях сетевых пользователей с целью последующего анализа и выявления возможных угроз.
3. UEBA (User and Entity Behavioral Analytics) — системы, позволяющие обнаруживать аномалии в действиях пользователей и работе самих корпоративных сетей [15].

Инцидентом информационной безопасности (кибератакой) называется любое незаконное, неразрешенное (в том числе политикой ИБ) или неприемлемое действие, которое совершается в информационной системе [16].

Чтобы отличить кибератаки от обычных операций в информационной системе, в рамках выполнения работы предлагается использовать многослойную модель глубокого обучения, которая объединяет результаты пяти прямых нейронных сетей с тремя полностью связанными скрытыми слоями.

Рассмотрим двоичную задачу обнаружения кибератак, где y= 1 обозначает атаку, y= 0 обозначает естественное событие.

Предположим, что уже представлено обучение N моделей глубокого обучения $m_l(x)$, l=1,…, N которые все лучше, чем случайные угадывания, то есть P(ml(x))=p>0,5.

Математическая модель глубокого обучения определяется формулой (1):

$$\begin{cases} m(x) = 1, \text{при } \sum_{l=1}^{N} \frac{m_l(x)}{N} > 0{,}5; \\ m(x) = 0, \text{в другом случае.} \end{cases} \quad (1)$$

Предположим, что N моделей глубокого обучения независимы. Также предположим, что новая функция хнов соответствует атаке, тогда вероятность того, что разработанная модель глубокого обучения предсказывает атаку, равна:

$$P\left(m(x_{нов})\right) = \\ = P\left(\frac{1}{N}\sum_{l=1}^{N} m_l(x_{нов}) > \frac{1}{2}\right) > \left(1 - e^{-2\left(p-\frac{1}{2}\right)^2 N}\right), \quad (2)$$

где последнее неравенство следует из неравенства Хёффдинга для случайных величин Бернулли.

Когда число N становится большим, вероятность в формуле (2) приближается к 1, и это показывает, что сложенная модель глубокого обучения может быть произвольно точной по мере увеличения количества усредненных моделей.

Прогнозируемая MSE многослойной модели глубокого обучения равна:

$$E(m(x_{нов}) - 1)^2 = \\ = P\left(\frac{1}{N}\sum_{l=1}^{N} m_l(x_{нов}) > \frac{1}{2}\right) \le e^{-2\left(p-\frac{1}{2}\right)^2 N}, \quad (3)$$

где, как и в предыдущем примере, последнее неравенство следует из неравенства Хёффдинга.

По мере увеличения числа усредненных моделей N прогнозируемая MSE модели глубокого обучения с накоплением может быть сколь угодно близкой к 0, как показано в (3).

Поскольку MSE прогнозирования отдельной модели фиксируется, этим можно доказать, что MSE прогнозирования составной модели глубокого обучения может быть сколь угодно малым по сравнению с индивидуальной моделью глубокого обучения.

Теоретический анализ основан на методах ансамблевого обучения, например, Adaboost и random forest. Метод Adaboost и случайный лес улучшают точность классификации отдельных деревьев, где также обсуждаются корреляции между отдельными моделями. На практике отдельные модели обучаются с использованием одного и того же набора данных, и поэтому отдельные модели коррелируются.

Для контроля защищенности и выявления нарушений ИС строится пять нейронных сетей. Структура сети «мотивирована» тем, что сети с большим количеством скрытых слоев обычно расширяют представленные функции и достигают большей способности в решении реальных проблем.

Функция активации для скрытых слоев — это функция (ReLU), в то время как функция активации для выходного слоя — это сигмоидальная функция и функция softmax для данных двух классов и данных нескольких классов соответственно.

Обозначим выход l- го слоя как al=(a_{l1},… a_{nl}), где n — количество нейронов в i- м слое.

Например, n=60 во втором слое первой сети. Первый слой будет входным, а последний — выходным.

Обозначим L как количество слоев.

Выход (l+1) — го слоя будет записан следующим образом:

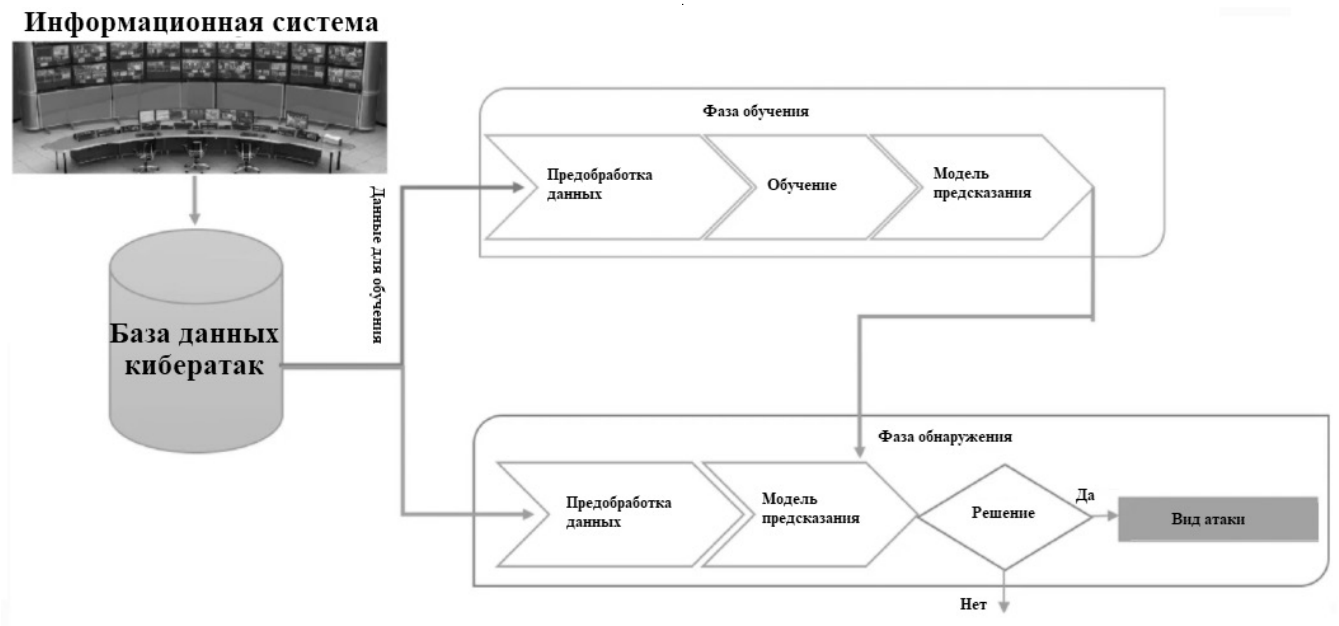

Рис. 2. Блок-схема предлагаемой процедуры контроля защищенности информационной системы

$$a^{l+1} = \sigma(W^{l+1}a^l + b^l), \quad (4)$$

где W^{l+1} — матрица mxn коэффициентов слоя (l+1);

m — количество нейронов слоя (l+1);

b^l — вектор смещения;

σ(x)=max(0, x) — функция активации.

Для скрытых слоев справедлива следующая формула:

$$\sigma(x) = \frac{1}{1+e^x}, \quad (5)$$

сигмовидная функция для двоичной классификации.

Обозначим через (x , y) одни наблюдаемые данные, где x — набор характеристик y= (y_1, …, y_c) — кодировка наблюдаемого события.

Для бинарной классификации, когда определяем, является ли событие кибератакой, используем бинарную кросс-энтропию в качестве функции потерь.

Для классификации на несколько классов, где также определяем тип атаки, мы используем перекрестную энтропию нескольких классов в качестве функции потерь.

В частности, функция потерь:

$$L(W,b) = \sum_{j=1}^{c} y_i \log\left(a_j^L\right). \quad (6)$$

На рисунке 2 показана блок-схема предлагаемой процедуры контроля защищенности информационной системы наземного комплекса управления с применением разработанной математической модели обучения нейронной сети.

Блок разделен на этап обучения и этап обнаружения. На этапе предварительной обработки данных удаляем отсутствующие значения и стандартизируем числовые функции.

На этапе обучения обучаем нейронную сеть и с использованием математической модели.

Наконец, обученная модель проверяется с использованием данных тестирования.

В долгосрочной перспективе точность повышается в процессе обучения, а это означает, что модель глубокого обучения постепенно изучила структуру данных и сходилась после завершения обучения [17,18].

В каждую эпоху стоимость вычислений стохастического градиентного спуска составляет приблизительно O(n, m), где n — количество выборок в эпоху, а m- количество параметров в сети, например количество весов и смещений в сети.

Следовательно, вычислительная нагрузка на обучение возрастает по мере увеличения количества эпох и выборок, количества нейронов в каждом слое и глубины сети. Обучение методам глубокого обучения

можно значительно ускорить с помощью современных устройств и программного обеспечения для параллельных вычислений.

Заключение

Таким образом, предполагается, что продемонстрирована многообещающая производительность комплексного подхода, основанного на глубоком обучении, для улучшения обнаружения вторжений для выявления нарушений информационной безопасности наземного комплекса управления для спутниковой сети связи.

Прогнозируется, что такой подход также позволяет обнаруживать широкие классы атак в ИС с использованием очень простого набора функций. Многослойный подход глубокого обучения обладает высокой производительностью обнаружения по сравнению с базовыми методами машинного обучения, а также с автономными моделями глубокого обучения.

ЛИТЕРАТУРА

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум. М.: КноРус, 2019. 432 с.
2. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем. М.: Инфра-М, 2018. 64 с.
3. Тархов, Д.А. Нейросетевые модели и алгоритмы. М.: Радиотехника, 2014. 643 с.
4. Олескин, А.В. Сетевые структуры в биосистемах и человеческом обществе.— М.: Едиториал УРСС, Либроком, 2015. 304 с.
5. Редько, В.Г. Эволюция, нейронные сети, интеллект: Модели и концепции эволюционной кибернетики. М: СИНТЕГ, 2017. 224 с.
6. Галушкин, А.И. Нейронные сети: история развития теории. М.: Альянс, 2015. 840 с.
7. Каллан, Р. Нейронные сети: Краткий справочник. М.: Вильямс, 2017. 288 с.
8. Zhang W., Zhang Z., Chao H.C., & Guizani M. Toward Intelligent Network Optimization in Wireless Networking: An Auto-Learning Framework. IEEE Wireless Communications, 26(3), 2019. pp.76–82.
9. Ширяев, В.И. Финансовые рынки: Нейронные сети, хаос и нелинейная динамика. М.: Ленанд, 2019. 232 с.
10. Hinton, G., Deng, L., Yu, D., Dahl, G.E., Mohamed, A.-R., Jaitly, N., Senior, A., Vanhoucke, V., Nguyen, P., Sainath, T.N., et al.: Deep neural networks for acoustic modeling in speech recognition: the shared views of four research groups. IEEE Signal Process. Mag. 29(6), 2012. pp. 82–97.
11. Ren, S., He, K., Girshick, R., Sun, J.: Faster R-CNN: towards real-time object detection with region proposal networks. In: Advances in neural information processing systems, 2015. pp. 91–99.
12. He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. In: IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016. pp. 770–778.
13. Wang, W., Harrou, F., Bouyeddou, B. et al. A stacked deep learning approach to cyber-attacks detection in industrial systems: application to power system and gas pipeline systems. Cluster Comput, 2021. 18 p.
14. Савельев Р.Н., Карцан И.Н. Основные методы выявления нарушения информационной безопасности по данным мониторинга наземного комплекса управления спутниковой сети // сборник Актуальные проблемы авиации и космонавтики / под общ. ред. Ю.Ю. Логинова; СибГУ им. М.Ф. Решетнева: в 3-х т.— Красноярск, 2021.— Т. 2.— С. 405–408.
15. Saveliev R.N., Kartsan I.N. Basic methods for detecting information security violations based on monitoring data of the satellite network ground control system // Tochnaya nayka.— 2022.— № 126.— pp. 4–6.
16. Савельев Р.Н., Карцан И.Н. Выявление отклонений информационной безопасности при мониторинге наземного комплекса управления спутниковой сети // Точная наука.— 2022.— № 125.— С. 2–4.
17. Ioffe, S., Szegedy, C.: Batch normalization: accelerating deep network training by reducing internal covariate shift. In: International Conference on Machine Learning, 2015. pp. 448–456.
18. Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., Anwar, A.: Ton iot telemetry dataset: a new generation dataset of iot and iiot for data-driven intrusion detection systems. IEEE Access 8, 2020. 25 p.

Журнал «Современная наука: актуальные проблемы теории и практики»