DOI 10.37882/2223-2966.2024.6-2.25

МОДЕЛЬ УПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЕМ ИНФОРМАЦИОННЫМ АТАКАМ В КИБЕРПРОСТРАНСТВЕ

MODEL OF MANAGEMENT FOR COUNTERING INFORMATION ATTACKS IN CYBERSPACE

A. Kolesnikov

Summary. The article is devoted to the study of current problems related to countering information attacks in cyberspace. During the research process, it was noted that it is advisable to use an evolutionary approach as the conceptual basis of the model. The author's version of a model for detecting an attack with false data injection in an industrial control system is presented. The basis of the developed model is a combination of the state estimation method of two convolutional neural networks (CNN-CNN) for selecting functions and building a reliable mechanism for identifying the actions of attackers.

Keywords: model, attack, cyberspace, neural network.

Колесников Антон Александрович
Санкт-Петербургский Политехнический университет Петра Великого,
anton.kolesnikov.science@mail.ru

Аннотация. Статья посвящена изучению актуальных проблем, связанных с противодействием информационным атакам в киберпространстве. В процессе исследования отмечено, что в качестве концептуальной основы модели целесообразно использовать эволюционный подход. Представлен авторский вариант модели обнаружения атаки с ложным внедрением данных в системе промышленного управления. Основу разработанной модели составляет комбинация метода оценки состояния двух сверточных нейронных сетей (CNN-CNN) для выбора функций и построения надежного механизма идентификации действий злоумышленников.

Ключевые слова: модель, атака, киберпространство, нейронная сеть.

В настоящее время большая часть экономической, коммерческой, культурной, социальной и правительственной деятельности, а также взаимодействие стран на всех уровнях, включая частных лиц, неправительственные организации, государственные и международные учреждения, осуществляется в киберпространстве. Жизненно важные и чувствительные инфраструктуры и системы либо сами являются частью киберпространства, либо контролируются, управляются и эксплуатируются через него, а большая часть информации, имеющей критическое значение, передается в это пространство или формируется в нем [1].

В данном контексте на фоне быстрого развития цифровой среды конвергенция цифровизации и киберугроз создает новые проблемы для организационной безопасности. Регулярно можно слышать новости, о предприятиях, которые платят огромные штрафы или даже прекращают деятельность из-за взлома их систем. В 2023 году количество кибератак во всем мире увеличилось на 125 % по сравнению с 2022 годом, а во время пандемии COVID-19 прирост составил 600 % [2]. Киберпреступность развивается быстрыми темпами, она включает в себя все: от кражи или растраты до взлома и уничтожения данных. Практически каждой отрасли приходится внедрять новые решения, а компаниям быстро адаптироваться к изменяющемуся цифровому ландшафту.

Хакерам становится все более выгодно осуществлять атаки и незаконное вторжение, а их методы и схемы действий становятся все более изощренными и опасными. Ожидается, что к 2025 году убытки от киберпреступности вырастут до 10,5 триллионов долларов в год. Потери, связанные с киберпреступлениями, включают в себя уничтожение данных, хищение денежных средств, снижение производительности, кражу интеллектуальной собственности, а также личных и финансовых данных, мошенничество, нарушение нормального хода дел после атаки, проведение судебной экспертизы, восстановление и удаление взломанных данных и систем, а также ущерб репутации.

Очевидно, что в таких условиях стремительно развивающаяся ситуация с киберугрозами требует принятия решительных мер. Наличие надежного плана управления рисками имеет решающее значение для того, чтобы помочь компаниям снизить подверженность кибератакам. Руководители бизнеса должны постоянно обновлять, совершенствовать и тестировать свои стратегии защиты в киберсреде для борьбы с различными вредоносными элементами, к числу которых относятся: программы-вымогатели и компрометация деловой электронной почты, фишинг, атаки вредоносного ПО, мошенничество в области социальной инженерии, кража паролей и т.д.

С учетом отмеченных обстоятельств особого внимания заслуживает внедрение проактивных систем управления кибербезопасностью, которые будут опираться на аналитический подход, позволяющий предотвратить взлом, либо обеспечить его быстрое обнаружение и устранение. Актуальность данной проблематики и предопределила выбор темы статьи.

Над обоснованием ключевых факторов, формирующие киберустойчивость организации к атакам трудятся такие авторы как: Рудзейт О.Ю., Добржинский Ю.В., Титанов В.М., Liyou Li, Hang Yang, Rongjun Cheng.

Четырехэтапный подход OM-AM (объект, модель, архитектура и механизм) к построению модели противодействия информационным атакам в киберпространстве, который позволяет разработчику включать в контур защиты абстрактный и конкретный уровень, описывают в своих публикациях Павленко Е.Ю., Степанов М.Д., Обухова А.С., Пияльцев А.И., Thomas J. Holt, Mae Griffith, Noah Turner, Emily Greene-Colozzi.

Анализ публикаций по теме исследования позволяет прийти к выводу, что на сегодняшний день существует достаточно большой массив моделей и методов, которые преимущественно сфокусированы на проблеме идентификации информационной атаки. Однако, некоторые отдельные моменты и проблемные аспекты требуют более детального анализа. Так, например, в уточнении нуждаются вопрос — какие возможности цифровизации способны обогатить структуру киберустойчивости на фоне постоянных изменений в цифровой экосистеме. Кроме того, в дальнейшем развитии нуждаются методы обнаружения кибератак с помощью алгоритмов неконтролируемого интеллектуального анализа данных.

Таким образом, цель статьи заключается в рассмотрении подходов к разработке модели управления противодействием информационным атакам в киберпространстве.

Прежде всего целесообразно отметить, что кибератака — это любая преднамеренная попытка украсть, раскрыть, изменить, отключить или уничтожить данные, приложения или другие активы посредством несанкционированного доступа к сети, компьютерной системе или цифровому устройству [3]. В целом кибератаки делятся на два типа: целевые и нецелевые. При нецелевых атаках злоумышленники без разбора атакуют как можно больше устройств, служб или пользователей. Их не волнует, кто является жертвой, поскольку существует ряд машин или сервисов с уязвимостями. Для этого применяются методы, использующие открытость Интернета. При целенаправленной атаке конкретная система или пользователь становится мишенью, поскольку злоумышленник проявляет особый интерес к ней по разным причинам. Подготовка к атаке может занять несколько месяцев, чтобы найти оптимальный путь для доставки эксплойта непосредственно в систему. Целенаправленная атака зачастую наносит больший ущерб, чем нецеленаправленная, поскольку она специально разработана для конкретного объекта.

Учитывая специфику и тенденции развития злонамеренной, криминальной активности в киберпространстве, основу большинства моделей управления противодействием информационным атакам в киберпространстве составляет эволюционный подход, который предполагает переход от обычных статических мер безопасности к тактике адаптивной защиты от киберугроз [4]. Схематично структура эволюционного подхода представлена на рис. 1.

Рис. 1. Структура эволюционного подхода к управлению противодействием информационным атакам в киберпространстве (составлено автором)

Рассмотрим практический пример реализации модели управления противодействием информационным атакам в киберпространстве на примере системы промышленного управления (ICS), которая представляет собой особый тип киберфизической системы, включающий в себя физические системы и объекты промышленных процессов, а также элементы SCADA, интеллектуальные датчики, промышленный Интернет вещей, сетевые ресурсы и анализ данных. Наиболее популярным типом кибератак на эти системы является атака с ложным внедрением данных (FDIA), которая предполагает внедрение ложных настроек (FSI) и ложных команд (FCI).

FDIA можно смоделировать математически с использованием следующего уравнения:

$$FalseData = D_{i,j} + F_{i,j}$$

где $D_{i,j}$ — исходный набор данных, а $F_{i,j}$ — инжектированные данные.

Объединение инжектированных данных с исходными данными приводит к появлению ложных данных. Здесь $F_{i,j}$ может быть любым из следующих вариантов:

— удаление данных из исходного набора данных, $D_{i,j}$;
— изменение данных в исходном наборе данных, $D_{i,j}$;
— добавление фальшивых данных к исходному набору данных, $D_{i,j}$.

Хотя в выше представленном уравнении рассматриваются данные, представленные в структурированном виде, атаки на вброс ложных данных можно рассматривать и для неструктурированных наборов.

Далее акцентируем внимание на оценке состояния, которая необходима для объединения измерений, полученных через сеть связи, и управления операционной деятельностью в интеллектуальной сети. Оценка состояния автоматически удаляет ошибочную информацию, вызванную случайными помехами, оценивает или предсказывает рабочее состояние системы и использует избыточность измерительного контура для повышения точности данных [5]. Опираясь на информацию, собранную в режиме реального времени с устройств, таких как блок фазовых измерений (см. рис. 2), оценка состояния направлена на анализ рабочих условий интеллектуальной сети. Напряжение на шинах, инжекция активной и реактивной мощности на каждой шине и комплексные потоки мощности в ветвях являются примерами типичных измерений.

Вектор состояния для системы с n шинами представлен следующим образом:

$$v = \left[v_1, v_2, v_3, \ldots, v_n \right]^T \left(v_i \in R \right)$$

где v_i обозначает переменную состояния на i-й шине, которая обычно включает угол напряжения или амплитуду напряжения. Рассмотрим вектор измерений z:

Вектор измерения для системы с n шинами записывается как:

$$z = \left[z_1, z_2, z_3, \ldots, z_n \right]^T \left(z_i \in R \right)$$

Для неидеальных датчиков существуют некоторые различия между значениями функции измерения и фактическими данными. Оценка состояния в реальной электроэнергетической системе с учетом ошибок измерений может быть определена как:

$$z = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix} = \begin{bmatrix} H_1\left(v_1, v_2, v_3, \ldots, v_n\right) \\ H_1\left(v_1, v_2, v_3, \ldots, v_n\right) \\ \vdots \\ H_m\left(v_1, v_2, v_3, \ldots, v_n\right) \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix}$$

Взаимосвязь между состояниями системы v и измерениями z может быть построена в виде линейного уравнения с использованием модели потока мощности постоянного тока, как показано ниже:

$$z = Hv + e$$

где e — вектор ошибок измерений (аддитивный шум), который обычно представлен гауссовым распределением, v — амплитуда и фазовый угол напряжения на шинах, z — вектор измерений, а H — топологическая матрица Якоби, которая отображает состояния системы, определяется следующей формулой — $H = \frac{\partial H(v)}{\partial v}$ и зависит от импеданса топологии сети.

Вопросы построения матрицы часто решаются с помощью алгоритма взвешенных наименьших квадратов. Квадратичная оптимизационная задача формулируется из формы оценки состояния, а оцениваемый линеаризованный вектор состояния v' задается следующим образом:

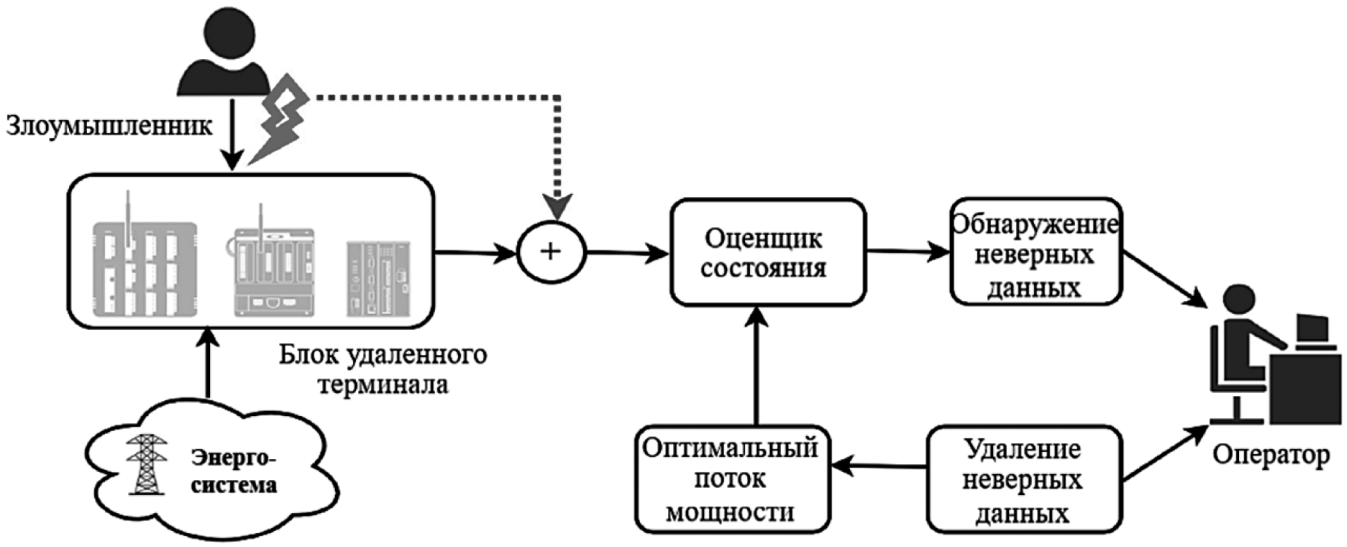

Рис. 2. Оценка состояния при кибератаке в интеллектуальной сети (составлено автором)

$$v' = \left(H^T H\right)^{-1} H_z^T$$

Неточные данные появляются в результате случайных ошибок измерений, в то время как ложные данные создаются злоумышленниками сознательно. Оценка состояния — распространенный метод обнаружения дефектных данных — неэффективен для идентификации FDIA, но отлично подходит для обнаружения неточных данных. FDIA позволяет злонамеренно вводить сгенерированные данные b в вектор измерения потока мощности как:

$$Z_{bad} = Nv + b + e$$

а вектор инжектированных ложных данных:

$$b = \left[b_1, b_2, b_3, \ldots, b_m\right]^T$$

$$Z_{bad} = z + b$$

Когда существуют ложные данные, вводимые злоумышленниками, b будет ненулевым вектором. Переменная состояния оценки v' изменится на v_F' из-за инъекции ложных данных, и будет $v_F' = v' + c$, где c — n-мерный ненулевой вектор. Если предположить, что вектор инжектированных данных Z_{bad} равен H_v, то b будет игнорироваться традиционным методом обнаружения, как было сказано выше. Это объясняется тем, что

$$\left\|Z_{bad} - Hv_F'\right\| = \left\|z + b - H\left(v' + c\right)\right\| = \left\|z - Hv'\right\|$$

Данные измерений должны быть проверены для обеспечения максимальной точности, а дефектные данные удалены. Традиционно для выявления дефектных данных используется тест 2-нормального остатка:

$$\|z - Hv\|^2 < \in$$

где 2 — порог обнаружения неточных данных. Неточные данные существуют и должны быть удалены до следу-

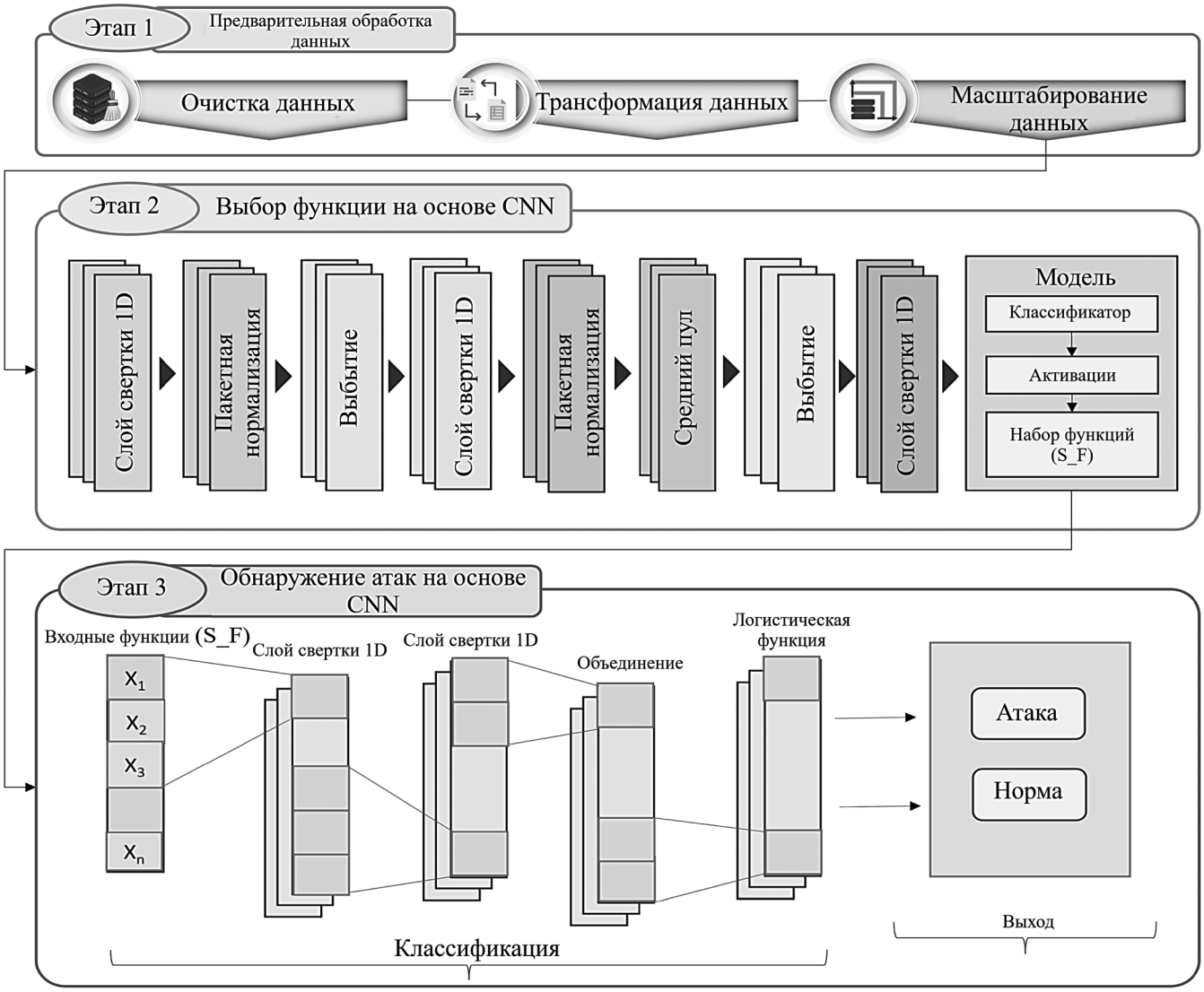

Рис. 3. Модель для выбора признаков и обнаружения FDIA в ICS на базе нейронных сетей

ющей итерации, если остаток измерений поднимается выше порога. Однако эти обычные методы обнаружения неточных данных не способны выявить скрытые и интеллектуальные атаки, такие как FDI.

В данном случае особого внимания заслуживают технологии искусственного интеллекта, в состав которых входят различные методы машинного обучения, глубокого обучения, анализа данных, эволюционные методы и методы нечеткой логики, позволяющие с требуемой степенью достоверности и точности обнаруживать FDIA.

На рис. 3 показана разработанная автором модель, которая использует архитектуру двойной конволюционной нейронной сети для выбора признаков и обнаружения FDIA в сетях ICS.

Представленная на рис. 3 модель направлена на использование возможностей CNN для автоматического выбора релевантных признаков из данных сетей ICS. CNN-CNN состоит из двух отдельных моделей CNN — одной для отбора признаков и одной для обнаружения атак, — которые работают вместе, дополняя друг друга, чтобы определить наиболее информативные признаки и точно выявить FDIA.

Таким образом, в статье представлена авторская модель управления противодействием информационным атакам в киберпространстве на примере обнаружения атаки с ложным внедрением данных в системе промышленного управления. Основу модели составляет комбинация метода оценки состояния двух сверточных нейронных сетей (CNN-CNN) для выбора функций и построения надежного механизма идентификации действий злоумышленников.

ЛИТЕРАТУРА

1. Осипенко А.А. Моделирование компьютерных атак на программно-конфигурируемые сети на основе преобразования стохастических сетей // Известия Тульского государственного университета. Технические науки. 2023. № 2. С. 274–281.
2. Ерохин С.Д. Анализ и разработка теоретико-игровых моделей обеспечения информационной безопасности критической информационной инфраструктуры // Системы синхронизации, формирования и обработки сигналов. 2023. Т. 14. № 6. С. 9–17.
3. Thavavel Vaiyapuri, K. Shankar Automated cyberattack detection using optimal ensemble deep learning model // Transactions on Emerging Telecommunications Technologies. 2023. № 56. P. 78–84.
4. Жуков М.М. Методологический подход к имитационному моделированию при исследовании практической эффективности систем защиты от сетевых кибератак // Вестник Воронежского института МВД России. 2022. № 1. С. 24–39.
5. He Wen, Faisal Khan Cybersecurity and process safety synergy: An analytical exploration of cyberattack-induced incidents // The Canadian Journal of Chemical Engineering. 2023. № 123. P. 87–94.

Журнал «Современная наука: актуальные проблемы теории и практики»