УДК 004.4 https://doi.org/10.51301/vest.su.2021.i6.14

[1]А. Асхатулы, [2]Д.Едилхан*, [1]Д. Бердышева
[1]Казахский Национальный Университет им. ал-Фараби, Алматы, Казахстан
[2]Астана IT-университет, Нур-Султан, Казахстан
*e-mail: yedilkhan@gmail.com

ИСПОЛЬЗОВАНИЕ МАШИННОГО ОБУЧЕНИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В современном мире существует глобальный дефицит специалистов в области кибербезопасности. Необходимость обучать и передавать экспертные знания о предмете стала настоящим вызовом для индустрии. Продукты традиционного и нетрадиционного образования на сегодняшний день не могут удовлетворить глобальный спрос на квалифицированных специалистов в сфере кибербезопасности, и данный тренд вряд ли измениться в ближайшие годы. Предприятия продолжают сталкиваться с большим количеством кибер-преступлений разного масштаба и вектора: фишинговые, сетевые, вредоносное ПО, отказ в обслуживании (DoS) и программы-вымогатели (ransomware). Многовекторные кибератаки приводят к ошеломляющему материальному и репутационному урону. Сообщество ИБ в постоянном поиске новых подходов к противостоянию непрерывным атакам злоумышленников. Тем временем, количество кибератак с каждым днем растет и становятся все более изощренными.

В эпоху больших данных и острой нехватки специалистов кибербезопасности, машинное обучение (МО) имеет все предпосылки стать эффективным решением. Целью данной статьи является анализ актуальных проблем в построении системы управления информационной безопасности (ИБ) и обсуждение примеров использования МО в процессах ИБ. В статье также отображены существующие проблемы и будущие направления развития МО в кибербезопасности.

Ключевые слова: машинное обучение, система информационной безопасности, безопасность сети, безопасность приложений, реагирование на события информационной безопасности.

Введение. Артур Самуэль в 1959 году ввел термин “машинное обучение” как способ обучения, дающий возможность компьютерам учиться без явного программирования [1]. Существует четыре широких категорий задач, решаемых с помощью алгоритмов МО: кластеризация, классификация, регрессия и извлечение правил [2]. Задача кластеризации состоит в том, чтобы сгруппировать схожие по определенным характеристикам данные, при этом увеличивая разрыв между группами. Задачей классификации и регрессии является получение категориального ответа или прогноза на основе входных данных. Задачи извлечения правил по своей сути различны, и их цель состоит в идентификации статистических связей в данных.

Алгоритмы МО могут отличаться в используемых подходах (например, дерево решений, метод опорных векторов, глубокое обучение, нейронные сети и алгоритмы продвинутой кластеризации), но предлагают уникальный способ анализа больших данных, где следующее эволюционное поколение алгоритмов обеспечивают более оптимальные решения [3].

Эффект бурного развития МО повлиял на ряд отраслей с интенсивным использованием данных, в том числе и на кибербезопасность. С помощью МО можно обрабатывать и анализировать большие объемы данных, генерируемые устройствами ИБ, совершенно новыми способами [3].

Автоматическое реагирование на события ИБ

На сегодняшний день устройства ИБ работают на основе сигнатурного мониторинга аномального поведения [4]. Сетевые устройства, как брандмауэры, системы защиты от вторжений и обнаружения вторжений, системы защиты пользовательских машин (антивирус, хост брандмауэр) генерируют сообщения о потенциальных злонамеренных действиях. Упомянутые технологии имеют одно ключевое ограничение: новые, неопознанные атаки не могут быть обнаружены, так как их сигнатура еще не хранится в локальной базе [4]. Своевременная локализация инцидента считается критичной задачей в этой ситуации. Для этого предприятия должны развивать адаптивный подход реагирования на новые атаки и в то же время продолжать эффективно справляться с известными атаками [5]. Новые стратегии управления событиями ИБ должны быть ориентированы на непрерывную обучаемость [5].

Современным операционным центрам безопасности (ОЦБ) и сетевым операционным центрам (СОЦ) необходимо изучить контекст атаки, чтобы реагировать на обнаруженные события. Аналитики кибербезопасности занимаются сбором информации о событиях криминалистической атаки из таких ресурсов, как packet capture, netflow и журналы устройств. Для автоматизации процессов управления событиями ИБ требуется наличие контекстуально и семантически богатой информации об инциденте [5]. В большинстве случаев аналитикам ОБЦ и СОЦ приходится сопоставлять и исследовать данные о событии вручную, которые в то же время хранятся на разных устройствах и могут предоставлять разрозненную информацию [6]. Решением проблемы должно быть использование единого репозитория, куда будут стекаться все данные ИБ, что облегчит их применение для обучения [6].

Существует ряд подходов управления событиями ИБ, которые позволяют адаптивное обучение. Анализ категориальных мер подобия, основанный на числовой таксономии, является одним из таких примеров [7]. Исследования показали, что с помощью числового и категориального анализа проблемы могут быть сгруппированы путем определения категориальных элементов, их признаков или атрибутов [7]. Кроме того, атрибуты могут быть измерены для определения релевантности признаков. Однако большинство проблем решаемых этим подходом являются бинарными по своей природе и их крайне сложно применить к событиям ИБ [7].

Авторы статьи [8] предлагают подход для анализа разнородных событий с помощью дистанционных функций, которые группируют события на основе категориальных и непрерывных атрибутов [8]. Данный подход обеспечивает контролируемый метод обучения классов информации, где каждый класс имеет набор категориальных и непрерывных атрибутов, которые можно оценить с помощью дистанционного обучения метрикам [8]. Предложенный подход очень хорошо работает для небольших и ограниченных наборов данных, но процесс управления событиями ИБ оперирует с большим количеством данных [8].

Модели нейронной сети были применены для своевременного реагирования на события ИБ, оповещения экспертов и генерации отчетов на основе критичности события и показали высокий уровень точности (90%) [9]. Для разработки модели нейронной сети в исследовании использовался фреймворк TensorFlow. В ходе тестирования модель определила и произвела реагирование на более 9 млн событий ИБ. Время, потраченное на анализ, сократилось на 78%. Вместо запланированных 2000 часов ручной работы, аналитики потратили бы 455 часов.

Машинное обучение в сетевой безопасности

Сетевая безопасность является краеугольным камнем в построении системы защиты ИБ. Проблемы сетевой безопасности могут быть сформулированы как задачи машинного обучения. К примеру, задача классификации может быть сформулирована как предсказание типа атаки безопасности: отказ в обслуживании, пользователь к корню (U2R), корень к локальной (R2L) или зондирование сети. Задачи регрессионного анализа могут быть сформулированы как предсказание сбоя в системе.

Алгоритмы МО в сфере сетевой безопасности базируются на подходе указанном в рисунке 1. К этапу сбора данных относится непосредственно сбор, создание и / или

определение набора данных и интересующих классов. Следом идет конструирование признаков для уменьшения размерности данных, что помогает снизить вычислительные затраты и повысить точность. Наконец, методы МО тщательно анализируют сложные взаимосвязи в данных и обучают модель.

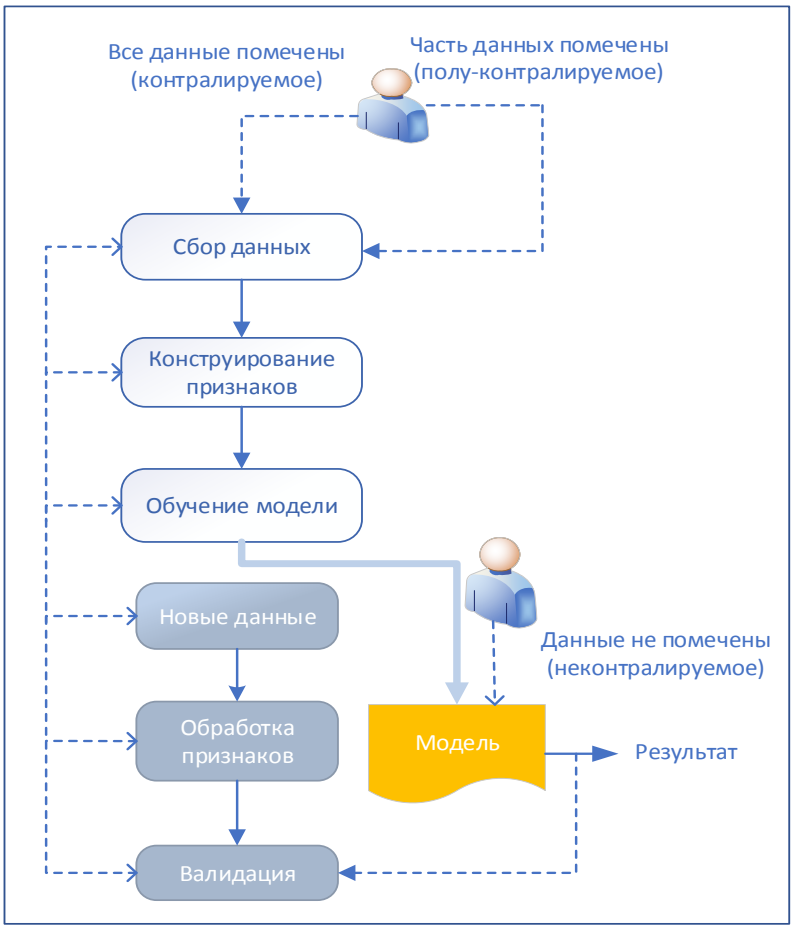

Рисунок 1. Основные составляющие общего подхода построения алгоритмов МО

Классификация трафика

Традиционно интернет трафик классифицируется по номеру порта, полезной нагрузке и конечной машине (host based). По причине использования динамического согласования портов, туннелирования и подмены номеров портов для общеизвестных приложений, классификация по номеру порта считается ненадежным и устарелым методом [10].

В свою очередь, классификация, основанная на полезной нагрузке, имеет широкое применение, хотя и требует значительных вычислительных ресурсов в работе с зашифрованными данными. Контролируемые (supervised) и неконтролируемые (unsupervised) типы МО успешно применяется для классификации трафика с высокой точностью.

Как правило, на практике для классификации трафика используется незашифрованная полезная нагрузка, но этот подход не работает для каналов с высокой скоростью передачи данных. Долгоживущий UDP трафик классифицируется контролируемым обучением, где полезная нагрузка проверяется случайным образом в окне наблюдения [11]. Все же данный способ не пользуется популярностью, так как чувствителен к размеру окна наблюдения. Классификация трафика на основе хоста тоже очень чувствительна к асимметрии маршрутизации.

В отличии от вышеупомянутых подходов, в методе классификации трафика на основе потока данных проверяется полный сеанс связи, который включает в себя все

последовательные однонаправленные пакеты в сети. Это наиболее широко изученный метод классификации трафика, использующий как контролируемые, так и неконтролируемые виды обучения. В контролируемом обучении чтобы достичь высокую точности используются алгоритмы МО, такие как оценка ядра (kernel estimation), нейронные сети (neural networks) и метод опорных векторов (SVM).

Зачастую невозможно получить полные данные обо всех сетевых приложениях. Следовательно, нецелесообразно ожидать, что все необходимые данные для классификации сетевого трафика будут доступны. Поэтому методы неконтролируемого обучения, где основным признаком является данные о потоке, были широко изучены с практической точки зрения.

Контролируемые методы обучения обеспечивают высокую точность классификации трафика, в то время как неконтролируемое обучение является более надежным способом. Симбиоз применения 2-х подходов классификаций сетевого трафика показали отличные результаты [13]. Контролируемое обучение может быть легко адаптировано для трафика нулевого дня. Модель легко переобучается для повышения точности в работе с данными, полученными из ранее неизвестных приложений. Последние достижения в области сетевых технологий расширяют возможности классификации трафика путем идентификации приложений и категорий QoS (Quality of Service) на основе SDN (Software Defined Networking) и NFV (Network Function Virtualisation). Несмотря на то, что некоторые предварительные работы в этой области достигли высокой точности, все еще необходимо провести более тщательное изучение их устойчивости, временной и пространственной стабильности и вычислительных затрат. Также крайне важно оценить пригодность этих технологий для классификации трафика чувствительных ко времени.

Управление неисправностями

Управление неисправностями включает в себя обнаружение, изоляцию и исправление аномального состояния сети. Для этого необходимо иметь полное представление о сети, подключенных к ней устройствах и приложениях. Последние достижения в области виртуализации делают сегодняшнюю сеть масштабным по размеру, сложности и высокой динамичности. Таким образом, устранение неисправностей становится все более сложной задачей в современных сетевых технологиях. Большинство подходов МО применяющиеся в управлении сетевыми сбоями используют разные методы контролируемого обучения. Процесс прогнозирования, обнаружения и локализации неисправностей в сети посредством контролируемого обучения сильно зависит от наличия обучающих данных. Дефицит данных о сбоях сети является общей проблемой в данном контексте [14].

В тестовой или моделируемой сети доступны как данные о работе сети в штатном режиме, так и данные о сбоях, тогда как в производственной сети данные о сбоях встречаются редко. Искусственная инъекция ошибок в сеть способствует получению необходимых данных [15], но внедрение ошибок в производственную сеть только для получения обучающих данных является неоправданно рискованным вариантом. Более того, синтезированные данные, сгенерированные в тестовой или моделируемой сети, могут не полностью отображать поведение производственной сети. Такие ограничения увеличивают вероятность того, что методы ML будут плохо обучены в незнакомой сети. В качестве решения вместо помеченных данных о сбоях, можно использовать неконтролируемое обучение, основанное на обнаружении изменений состояния сети. Однако неконтролируемое обучение требует больше времени для схождения (converge), чем контролируемые подходы, потенциально пропуская любой сбой, возникающий до схождения. Таким образом, потенциальное направление будущих исследований заключаться в изучении комбинации контролируемого/ неконтролируемого обучения и обучения с подкреплением (Reinforcement Learning) для устранения неисправностей сети.

Безопасность приложения и машинное обучение

Веб-серверы и веб-приложения широко используются в различных предприятиях и подвергаются многочисленным атакам. Разработчикам веб-приложений необходимо создавать системы устойчивыми к известным атакам. При реализации успешной атаки крайне важно вовремя обнаружить и локализовать последствия. Данные о кибератаке в последствии будут использоваться для реагирования на инцидент, ограничения ущерба, судебного преследования и предотвращение будущих атак.

Обнаружение вторжения является одним из основных методов, предназначенных для выявления и предотвращения вредоносных действий в системе [16]. Этот метод имеет два основных класса: обнаружение злонамеренных действий и обнаружение аномалий. Обнаружение злонамеренных действий идентифицирует атаки на веб-приложения путем сравнения текущей активности с ожидаемыми действиями злоумышленника, обычно с использованием алгоритмов сопоставления. Напротив, подход обнаружения аномалий изучает поведение пользователя, будь то клиент или сервер, и определяет, является ли поведение нормальным или аномальным, часто с использованием методов машинного обучения.

Ряд исследований продемонстрировали усовершенствованный метод обнаружения вторжений с помощью машинного обучения. Например, в статье [17] были представлены различные алгоритмы машинного обучения такие как (random forest), логистическая регрессия (logistics regression), дерево решений (decision trees), AdaBoost и стохастический градиентный спуск (stochastics gradient descent), которые используются для построения систем обнаружения вторжений. Авторы создали экспериментальную среду для сравнения производительности некоторых методов машинного обучения, работающих на наборе данных HTTP CSIC 2010 [18], который содержит сгенерированный веб трафик в электронной коммерции. Результаты исследования показали, что логистическая регрессия является оптимальным методом обучения среди всех исследованных методов, показав приемлемую производительность и высочайшую точность.

Заключение. В статье были рассмотрены примеры использования алгоритмов МО в решении задач ИБ, таких как реагирование на событие ИБ, обеспечение сетевой безопасности и безопасности приложения. Было выявлено, что оба типа обучения модели (контролируемое и неконтролируемое) использовались в исследованиях и проявили свои сильные и слабые характеристики. Идеальным решением во многих случаях является применение комбинации из этих подходов. Результаты исследований показывают, что основной проблемой прикладного применения МО в процессах ИБ является нехватка данных для обучения моделей. В будущем авторы данной статьи планируют обучить математическую модель и применить ее в целях решения общеизвестной проблемы в построении защиты систем ИБ.

REFERENCES

[1] Puget JF. What is machine learning? (IT best kept secret is optimization). 2016. https://www.ibm.com/developerworks/community/ What_Is_Machine_Learning.

[2]Brownlee J. Practical Machine Learning Problems. 2013. https://machinelearningmastery.com/practical-machine-learning-problems/

[3]Ahn CW, Ramakrishna RS. Qos provisioning dynamic connection-admission control for multimedia wireless networks using a hopfield neural network. IEEE Trans Veh Technol. 2004;53(1):106–117

[4]W. Lynn, "Defending a new domain: the Pentagon's cyberstrategy." Foreign Affairs 89, no. 5 (2010): 97-108.

[5]K . Thakur, S. Kopecky, M. Nuseir, et al. "An analysis of information security event managers." In Cyber Security and Cloud Computing (CSCloud), 2016 IEEE

[6]Bayer, Ulrich, Paolo Milani Comparetti, Clemens Hlauschek, Christopher Kruegel, and Engin Kirda. "Scalable, Behavior-Based Malware Clustering." In *NDSS*, vol. 9, pp. 8-11. 2009.

[7]T. Bhavani, M. Kantarcioglu, K. Hamlen, et al. "A Data Driven Approach for the Science of Cyber Security: Challenges and Directions." In Information Reuse and Integration (IRI), 2016 IEEE 17th International Conference on, pp. 1-10. IEEE, 2016

[8]M. Huang, W. Lin, C. Chen, et al. "Data preprocessing issues for incomplete medical datasets." Expert Systems 33, no. 5 (2016): 432-438.

[9]J. Fraley, J. Cannady. The Promise of Machine Learning in Cybersecurity.), SouthestCon, IEEE, 2016

[10] Bernaille L, Teixeira R. Implementation issues of early application identification. Lect Notes Compu Sci. 2007;4866:156.

[11] Finamore A, Mellia M, Meo M, Rossi D. Kiss: Stochastic packet inspection classifier for udp traffic. IEEE/ACM Trans Netw. 2010;18(5):1505–15.

[12] Wang R, Liu Y, Yang Y, Zhou X. Solving the app-level classification problem of p2p traffic via optimized support vector machines. In: Intelligent Systems Design and Applications, 2006. ISDA'06. Sixth International Conference on, IEEE, vol 2; 2006. p. 534–9.

[13] Erman J, Mahanti A, Arlitt M, Cohen I, Williamson C. Offline/realtime traffic classification using semi-supervised learning. Perform Eval. 2007a;64(9):1194–213.

[14] Alpaydin E. Introduction to Machine Learning, 3rd ed. Cambridge: MIT Press; 2014.

[15] Lu X, Wang H, Zhou R, Ge B. Using hessian locally linear embedding for autonomic failure prediction. In: Nature & Biologically Inspired, Computing, 2009. NaBIC 2009. World Congress on. IEEE; 2009. p. 772–6.

[16] Khan, Javed Akhtar, and Nitesh Jain. "A Survey on Intrusion Detection Systems and Classification Techniques." *IJSRSET* 2.5 (2016): 202-208

[17] Pham, T.S., Hoang, T.H. and Vu., V.C. "Machine learning techniques for web intrusion detection—A comparison.‖ *Eighth International Conference on Knowledge and Systems Engineering (KSE),*. IEEE, 2016.

[18] Giménez, C.T., Villegas, A.P., and Marañón, G.A., ―HTTP Dataset CSIC 2010,‖ CSIC (Spanish Research National Council), 2012, http://www.isi.csic.es/dataset/

[1]А. Асхатулы, [2]Д. Еділхан*, [1]Д. Бердышева
[1]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
[2]Астана IT-университеті, Нұр-Сұлтан, Қазақстан
*e-mail: yedilkhan@gmail.com

МАШИНЫЛЫҚ ОҚЫТУ ӘДІСТЕРІНІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЛАСЫНДАҒЫ ҚОЛДАНЫСЫ

Аңдатпа. Бүгінгі таңда әлемде ақпараттық қауіпсіздік (АҚ) саласындағы мамандардың тапшылығы байқалуда. Киберқауіпсіздік мамандарын дайындау қоғам үшін нағыз сынаққа айналды. Алайда дәстүрлі және дәстүрлі емес білім беру әдістері білікті мамандарға деген сұранысты қанағаттандыра алмауда, бұл үрдіс жақын арада өзгеруі екіталай. Кибершабуылдардың саны күннен күнге артып, ауқымы мен шабуыл векторы сан түрлі болып келуде: фишинг, желіге шабуыл, зиянды бағдарламалар, DoS, ransomware бағдарламалары, т.б. Жан-жақты кибершабуылдар мекемелерге қаржылай және беделдік нұқсан келтіруін жалғастыруда. Ақпараттық қауіпсіздік қауымдастығы осындай шабуылдарға қарсы тұрудың жаңа тәсілдерін іздеуде, ал кибершабуылдардың саны мен күрделілігі күн сайын артып келе жатыр.

Кең ауқымды ақпараттың пайда болуы және киберқауіпсіздік саласындағы мамандардың тапшылығы дәуірінде, машиналық оқыту (МО) әдістері осы саладағы тиімді шешімдердің біріне айналуына мүдделі. Мақаланың мақсаты АҚ басқару жүйесіндегі қиыншылықтарды талдау және МО әдістерінің АҚ процестерінде қолданылуын сипаттау. Мақалада сондай-ақ МО АҚ саласында қолданудың бүгінгі таңдағы қиыншылықтары мен болашақ бағыттары көрсетілген.

Негізгі сөздер: машиналық оқыту, ақпараттық қауіпсіздік жүйесі, желінің қауіпсіздігі, бағдарламалық жасақтамалырдың қауіпсіздігі, қауіпсіздік оқиғаларына әрекет ету.

[1]A. Askhatuly, [2]D. Yedilkhan*, [1]D. Berdysheva
[1]al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]Astana IT-University, Nur-Sultan, Kazakhstan
e-mail: yedilkhan@gmail.com

USE OF MACHINE LEARNING IN INFORMATION SECURITY

Abstract. Global shortage of cybersecurity experts is becoming emerging trend in Information Security (IS) domain. Traditional and non-traditional education approaches are not able to supply global demand for cybersecurity talents, and this trend is unlikely to change in the coming years. Companies are experiencing a huge number of cyber-attacks of various scale and vector: phishing, network attacks, malware, denial of service (DoS) and ransomware. The effect of multi vector cyber-attacks could result in tremendous financial and reputational damage for the companies. Information security community is constantly looking for new approaches to combat with ever-growing number of cyber-attacks.

In an era of big data and a shortage of cybersecurity talents, machine learning (ML) has all the prerequisites to become one of the most efficient solutions in this field. The purpose of this article is to analyze current issues of IS management system and discuss practical use of ML in several IS processes. The article also discusses current challenges and future developments of ML in cybersecurity.

Keywords: machine learning, information security system, network security, application security, response to information security events.

.