Инженерный вестник Дона, №4 (2019)
ivdon.ru/ru/magazine/archive/n4y2019/5833

Информационная безопасность в робототехнике

М.С. Халиев, Х.Х. Пахаев

Чеченский государственный университет

Аннотация: В данном обзоре рассматривается, что такое искусственный интеллект, представляет ли он какую-либо опасность для людей, какие есть способы «завладеть» той или иной технологией контроля промышленных роботов. Как по этому поводу высказываются ученые и ведущие специалисты по информационным технологиям и физике.
Ключевые слова: информационные технологии, безопасность, взлом, робототехника, искусственный интеллект, угроза, уязвимость.

Что же такое искусственный интеллект? Искусственный интеллект (ИИ) – это сфера информатики, которая изучает интеллектуальные возможности средствами вычислительных технологий.

Термин появился в 1956 г. на семинаре в Стэндфордском университете в США. Семинар был направлен на изучение логических задач с использованием информационных технологий (ИТ).

С каждым годом искусственный интеллект развивается все быстрее и быстрее. Согласно прогнозам глобальная выручка компаний, которые занимаются разработкой и продвижением ИИ, вырастет с 2018 до 2025 года в 12 раз – с $7,3 до $89 миллиардов.

В настоящее время, ИИ пользуются в здравоохранении, автомобилестроении, в промышленных целях, голосовых ассистентах и в многих других сферах жизнедеятельности [1].

Как обучается ИИ? Двумя способами – машинным обучением и глубоким обучением.

Машинное обучение — это своего рода программы и алгоритмы, которым предоставляется информация, и с помощью заложенных алгоритмов

принимают те или иные решения. Собирая все больше информации, алгоритм учится и делает каждый следующий вывод более точным [2].

Глубокое обучение – с использованием искусственных нейронных сетей. ИИ учится понимать и разбирать данные, которые не были до этого структурированы, например, видео, изображения, звуки [3]. ИИ собирает информацию и обрабатывает его, выполнение этих действий способствует принятию решения.

С помощью чего ИИ становится умнее? Топливом для ИИ является – информация. Чем больше информации – тем умнее ИИ. Ум и скорость обработки ИИ растет прямо пропорционально количеству информации, которая поступает на его обучение [4]. С 2015 года было создано 90% информации, которым мы пользуемся по сей день (это около 10 зеттабайт памяти). По прогнозам, к 2020 году это число достигнет 20 зеттабайт, а к 2025 году, объемы достигнут аж 180 зеттабайтов. В 1 зеттабайте 1 миллиард терабайт [5][6].

Использование ИИ в промышленных целях и угроза работникам и предприятию. Три закона робототехники – свод правил, которые обязательно должны быть использованы при создании роботов [7], звучат они так:

«Робот не может причинить вред человеку или своим бездействием допустить, чтобы человеку был причинен вред.» (Айзек Азимов рассказ «Хоровод» 1942 года)

«Робот должен повиноваться всем приказам, которые дает человек, кроме тех случаев, когда эти приказы противоречат Первому Закону.» (Айзек Азимов рассказ «Хоровод» 1942 года)

«Робот должен заботиться о своей безопасности в той мере, в которой это не противоречит Первому или Второму Законам.» (Айзек Азимов рассказ «Хоровод» 1942 года)

Роботы и коботы (от сочетания слов collaborative bots) – два вида «железяк» которые помогают людям делать их работу, или вовсе заменяют человеческий труд. Главное отличие коботов от роботов – это то, что коботы работают совместно с людьми, в то время как роботы работают сами, исполняя алгоритмы, которые прописаны разработчиками. Роботы – силовые станции, они ограждены заборами и клетками для безопасности людей, они занимаются опасной работой, такой как поднятие тяжестей, разминирование территории и прочее [4][8].

Исследователи из IOActive обнаружили почти 50 уязвимых мест в коде промышленных коботов. Используя данные уязвимости, можно навредить рабочим или устроить шпионаж. Машины можно дистанционно контролировать, изменив их конфигурацию, например, если в них установлены камера и микрофон, можно делать промышленных шпионаж или изменить настройки безопасности [9], чтобы разрешить им покидать те зоны, которыми они были ограничены, также можно отключать датчики, которые выключают кобота при соприкосновении с людьми [10].

Возникает вполне здравый вопрос: как можно взломать роботов, и почему нельзя это предотвратить? Большинство современных технологий связаны через интернет. Сделано это для удобства управления. Допустим, роботы-пылесосы, которые встречаются все чаще и чаще. Некоторые из них, такие как iRobot Roomba i7, можно контролировать через телефон, соответственно, они должны быть подключены к интернету, и исходя из этого, их можно взломать [11] [12]. Любое устройство, любое ПО, которые тем или иным способом подключены к интернету считаются уязвимыми для взлома. Про локальное подключение и речи быть не может. Даже если код идеален и его практически невозможно взломать – нельзя забывать о железе, к которой тоже можно найти свой путь взлома. К примеру – перегрузка определенного модуля, перезапуск всего железа и т.д. [13]

Стивен Хокинг (английский физик-теоретик, космолог, писатель) высказал свою точку зрения по поводу ИИ и робототехники, он отметил, что существующие формы ИИ на сегодняшний день, доказали свою полезность людям, но также Хокинг опасается того, что человечество создаст что-то такое, что превзойдет своего создателя.

«Такой разум возьмет инициативу на себя и станет сам себя совершенствовать со все возрастающей скоростью. Возможности людей ограничены слишком медленной эволюцией, мы не сможем тягаться со скоростью машин и проиграем», - сказал Хокинг [15].

Но не все придерживаются такой точки зрения.

«Я думаю, что мы останемся хозяевами создаваемых нами технологий еще очень и очень долгое время, и они помогут нам решить многие мировые проблемы», - так считает Ролло Капентер, создатель веб-приложения Cleverbot (ПО Cleverbot неоднократное количество раз проходил тест Тьюринга, обманув людей).

«Мы не можем с уверенностью сказать, что произойдет, когда машины превзойдут нас интеллектом. Следовательно, мы не можем предсказать, и как они поведут себя: станут ли они нам помогать, нас игнорировать или же рано, или поздно нас уничтожат», - полагает Капентер.

А вот Илон Маск, предприниматель, основатель SpaceX и Tesla, придерживается мнения Хокинга, более того, он опасается искусственного интеллекта даже сейчас.

«Роботы могут начать войну, выпуская фейковые новости и пресс-релизы, подделывая учетные записи электронной почты и манипулируя информацией. Перо сильнее меча», - подчеркнул Маск [16].

Выводы

Искусственный интеллект и машинное обучение являются продуктами науки и гениального воображения. Хотя, сама идея, что машины могут

«думать» и выполнять умные действия наряду с людьми насчитывает тысячи лет, к примеру, големы и алхимия из прошлого. Современные технологии позволяют нам развивать когнитивные процессы, вовлекая их всё больше в наши научные и бытовые сферы жизни. Тревога людей по поводу «восстания» машин тоже не беспочвенна, любой робот, содержащий вирусный код, опасен для окружающих, поэтому значение специалистов по информационной безопасности для проектирования тотальной защиты программного содержания роботов очень велико для общей безопасности.

Литература

1. Менциев А.У., Анализ фишинговых атак как вида социальной инженерии. В сборнике: Наука и молодежь Всероссийская научно-практическая конференция студентов, молодых ученых и аспирантов. 2016. С. 391-394.

2. Инвестиции в будущее: искусственный интеллект. – URL: vc.ru/finance/46776-investicii-v-budushchee-iskusstvennyy-intellekt

3. Искусственный интеллект - угроза или помощник для человечества? – URL: bbc.com/russian/features-38931070

4. Роботы и коботы: 5 отличий. – URL: knn-systems.com/roboty-i-koboty-5-otlichij/

5. Три закона робототехники. – URL: ru.wikipedia.org/wiki/Три_закона_роботехники

6. Килюшева, Е. and Гнедин, Е. (2017). Как хакеры атакуют веб-приложения: боты и простые уязвимости. Securitylab.ru. URL: securitylab.ru/analytics/485977.php

7. Черемных, В. (2017). Виды хакерских атак. It-black.ru. URL: it-black.ru/vidy-khakerskikh-atak/

8. TAdviser.ru. (2019). Эксперты Лаборатории Касперского назвали общее число хакеров. URL: tadviser.ru/index.php/Статья:Хакеры

9. Semantica.in. (2017). Что такое вредоносный код. URL: semantica.in/blog/chto-takoe-vredonosnyj-kod.html

10. Revisium.com. (2018). Как искать вредоносный код без антивирусов и сканеров. URL: revisium.com/kb/find_malware_without_scanners.html

11. It-click.ru. (2016). Виды хакерских атак на веб-ресурсы. URL: it-click.ru/articles/web-studio/hacking-web-site.aspx

12. Mentsiev A.U., Dzhangarov A.I. VoIP security threats // Инженерный вестник Дона, 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5636

13. Mentsiev A.U., Supaeva Kh.S. VoIP techniques // Инженерный вестник Дона, 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5609

14. Positive Technologies. (2016). Атаки на веб-приложения. URL: ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Applications-Attacks-rus.pdf

15. Хокинг: искусственный интеллект - угроза человечеству. – URL: bbc.com/russian/science/2014/12/141202_hawking_ai_danger

16. Человечество в опасности: Илон Маск призвал регулировать искусственный интеллект. – URL: forbes.ru/tehnologii/347945-chelovechestvo-v-opasnosti-ilon-mask-prizval-regulirovat-iskusstvennyy-intellekt

References

1. Mentsiyev A.U., Analiz fishingovykh atak kak vida sotsial'noy inzhenerii [Analysis of phishing attacks as a type of social engineering]. V sbornike: Nauka i molodezh' Vserossiyskaya nauchno-prakticheskaya konferentsiya studentov, molodykh uchenykh i aspirantov. 2016. pp. 391-394.

2. Investitsii v budushcheye: iskusstvennyy intellect [Investing in the future: artificial intelligence]. URL: vc.ru/finance/46776-investicii-v-budushchee-iskusstvennyy-intellekt

3. Iskusstvennyy intellekt - ugroza ili pomoshchnik dlya chelovechestva? [Artificial intelligence - a threat or an assistant for humanity?]. URL: bbc.com/russian/features-38931070

4. Roboty i koboty: 5 otlichiy [Robots and cobots: 5 differences]. URL: knn-systems.com/roboty-i-koboty-5-otlichij/

5. Tri zakona robototekhniki [Three laws of robotics]. URL: ru.wikipedia.org/wiki/Tri_zakona_robotekhniki

6. Kilyusheva Ye. and Gnedin Ye. (2017). Kak khakery atakuyut veb-prilozheniya: boty i prostyye uyazvimosti [How hackers attack web applications: bots and simple vulnerabilities.]. Securitylab.ru. URL: securitylab.ru/analytics/485977.php

7. Cheremnykh, V. (2017). Vidy khakerskikh atak [Types of hacker attacks]. It-black.ru. URL: it-black.ru/vidy-khakerskikh-atak

8. TAdviser.ru. (2019). Eksperty Laboratorii Kasperskogo nazvali obshcheye chislo khakerov [Kaspersky Lab experts have named the total number of hackers]. URL: tadviser.ru/index.php/

9. Semantica.in. (2017). Chto takoye vredonosnyy kod [What is malicious code]. URL: semantica.in/blog/chto-takoe-vredonosnyj-kod.html

10. Revisium.com. (2018). Kak iskat' vredonosnyy kod bez antivirusov i skanerov [How to search for malicious code without antiviruses and scanners]. URL: revisium.com/kb/find_malware_without_scanners.html

11. It-click.ru. (2016). Vidy khakerskikh atak na veb-resursy [Types of hacker attacks on web resources]. URL: it-click.ru/articles/web-studio/hacking-web-site.aspx

12. Mentsiev A.U., Dzhangarov A.I. Inženernyj vestnik Dona (Rus). 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5636

13. Mentsiev A.U., Supaeva Kh.S. Inženernyj vestnik Dona (Rus). 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5609

14. Positive Technologies. (2016). Ataki na veb-prilozheniya [Attacks to web applications]. URL: ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Applications-Attacks-rus.pdf

15. Khoking: iskusstvennyy intellekt - ugroza chelovechestvu [Hawking: artificial intelligence - a threat to humanity]. URL: bbc.com/russian/science/2014/12/141202_hawking_ai_danger

16. Chelovechestvo v opasnosti: Ilon Mask prizval regulirovat' iskusstvennyy intellect [Humanity is in danger: Ilon Musk called for regulating artificial intelligence]. URL: forbes.ru/tehnologii/347945-chelovechestvo-v-opasnosti-ilon-mask-prizval-regulirovat-iskusstvennyy-intellekt