|  |  |  |
| --- | --- | --- |
| **ОТЧЕТ**  **о научно-исследовательской работе за 2 семестр 2022/2023 учебного года** | | |
| **ФИО студента** | | Самойлов Павел Александрович |
| **Факультет, группа** | | *Центр дополнительного, дополнительного профессионального и онлайн-образования "Пуск"* |
| **Базовая организация, кафедра** | | *Центр дополнительного, дополнительного профессионального и онлайн-образования "Пуск"* |
| **Тема НИР** | | **"Адаптация и совершенствование моделей глубокого обучения на базе встраиваемых систем для решения задач обеспечения безопасности устройств, реализующих технологии компьютерного зрения"** |
| **Текущее состояние НИР за семестр (проделанная работа и полученные результаты)** | | ***Цели, задачи, проблема и гипотеза исследования.***  Многофункциональность, практическая полезность и общепризнанная эффективность Интернета вещей закономерно определяют актуальную тенденцию активного развитию данного направления. Ежегодно фиксируется рост количества «умных» устройств, при этом совершенствуются датчики, встраиваемые системы, сетевые технологии и модели взаимодействия. Благодаря прогрессу в рассматриваемой области стали возможны технологические комплексы «Умный дом» и «Умный город», усовершенствованы системы навигации автономных транспортных средств, решены многие проблемы своевременной профилактики промышленного оборудования и многое другое. Однако бурное развитие Интернета вещей неизбежно привело к возникновению новых угроз информационной безопасности. Кратко суть проблемы можно сформулировать следующим образом. Умные устройства самостоятельно получают, обрабатывают и обмениваются информацией, при необходимости передают ее на устройства пользователей, в том числе используя сетевые или облачные технологии. При этом целый ряд узловых элементов Интернета вещей подвержены риску несанкционированного доступа. Встраиваемые системы не являются исключением, более того они могут быть главной целью атаки, поскольку оснащены автономными вычислительными и запоминающими устройствами. Злоумышленники могут получить доступ к государственной и коммерческой тайне, личной информации пользователей, в том числе персональным данным воздействуя непосредственно на встраиваемую систему умного устройства, не тратя время на обход сложных систем защиты сайтов, серверных и облачных хранилищ. Исследователи и разработчики умных устройств признают, что в погоне за эффективностью основного функционала устройства и встраиваемой системы в эволюционном процессе вопросы безопасности отодвигались на второй план. На текущем этапе развития и интеграции Интернета вещей практически во все сферы жизнедеятельности общества игнорировать вопросы безопасности встраиваемых систем стало абсолютно невозможно. Актуальность проблемы общепризнана мировым сообществом, выходы из ситуации ищут уже не только корпорации, производящие умные устройства и встраиваемые системы, но и государства активно начали разрабатывать технологические и юридические меры, направленные на минимизацию рисков использования технологий Интернета вещей.  Науки и технологии не стоят на месте. На сегодняшний день успешно реализуются множество решений обозначенный проблемы, но технологии Интернета вещей не стоят на месте и методы обеспечения безопасности должны развиваться параллельно с ними. На наш взгляд одним из наиболее эффективных направлений в рассматриваемой сфере является совершенствование программах средств защиты. Тем более, что встраиваемые системы имеют возможность автономного выполнения кода. Речь идет о программировании встраиваемой системы с имплементацией моделей машинного обучения. Традиционно это задача сводится к внедрению алгоритмов выявления аномалий в работе устройств и сетей. Однако реализация таких алгоритмов на практике вызывает определенные трудности. Так для достижения наибольшей эффективности в обеспечении безопасности, необходимо учитывать целый ряд технологических особенностей встраиваемых систем, из которых в первую очередь следует упомянуть: особенности работы датчиков, необходимость обеспечения основного функционального алгоритма устройства (например детектирования объектов), ограничение вычислительных мощностей, проблемы энергосбережения, недостаточность и изменчивость данных и т. д. Указанные особенности существенно влияют на и выбор конкретной модели машинного обучения, как правило выбирается наиболее простой алгоритм. Простой не значит плохой. В научных исследованиях последних лет есть немало работ, где достаточно высокие показатели выбранной метрики получают программы, определяющие аномалии по статистическим формулам, не задействуя машинное обучение. Что же касается машинного обучения, то здесь мнения в науке существенно отличаются, ряд авторов говорят эффективности классических алгоритмов машинного обучения для выявления аномалий во встраиваемых системах (например, Random Forest, KNN, Support Vector Machine). Однако результаты последних исследований в рассматриваемой области свидетельствуют о небольшом, но се же преимуществе нейронных сетей глубокого обучения над классическими алгоритмами. Отмечая этот факт, ученые объективно указывают на ряд проблем, возникающих при использовании глубоких нейронных сетей. Выделяют низкую скорость обучения, значительные вычислительные затраты, высокое количество ложных срабатываний и отсутствие научно-обоснованных методик выбора архитектуры сети и гиперпараметров.  Добавим к сказанному еще два фактора, которые имеют принципиальное значение для выбора программных методов и защиты информации во встраиваемых системах. Речь идет о назначении устройства и технологиях, обеспечивающих его функционирование. Сегодня в зоне высокого риска находятся устройства, работающие с фото и видео информацией, в том числе обрабатывающих ее при помощи технологий компьютерного зрения. Вместе с тем ущерб от неправомерного доступа к личной информации, обрабатываемой во встраиваемых системах или от целенаправленного изменения компьютерной информации, задействованной в механизме принятия системой решений в автономном режиме может быть непоправимым.  С учетом изложенного цель настоящего исследования состоит в поиске наиболее эффективных вариантов применения глубоких нейронных сетей для решения задач обеспечения безопасности встраиваемых систем, использующих технологии компьютерного зрения.  Для поставленной цели необходимо последовательное решение нескольких задач:   1. Необходимо детально рассмотреть элементы типовой модели системы Интернета вещей, использующей встраиваемые системы, обеспечивающие реализацию технологий компьютерного зрения. Составить схему модели, изучить потоки данных, их источники, форму и способы передачи на каждой стадии работы устройств в системе. 2. С учетом предыдущего пункта составить модель в которой предусмотреть классификацию угроз безопасности и возможные сценарии атак 3. Определить ключевые узлы в алгоритме работы системы, где есть потребность в реализации защитных механизмов 4. С учетом особенностей обрабатываемых данных и функционирования встраиваемых систем разработать и реализовать модели машинного обучения на основе глубоких нейронных сетей, способные эффективно выявлять аномалии и решать другие задачи, необходимые для обеспечения безопасности. Обосновать выбор архитектуры сети и используемого программного обеспечения 5. Провести тестирование моделей с использованием специализированных сервисов. Реализовать оптимизацию гиперпараметров.   Рабочую гипотезу исследования можно сформулировать следующим образом. Для обеспечения информационной безопасности устройств, реализующих технологии компьютерного зрения наиболее рациональным решением, будет, использование глубоких нейронных сетей. Нейронные сети благодаря их способности работать с разнообразными данными способны эффективно выявлять различные виды угроз. Для этого необходимо подбирать оптимальную архитектуру, гиперпараметры, а также необходимо максимально использовать возможности основного алгоритма компьютерного зрения, например, для активации протокола безопасности при физическом контакте с устройством). В идеале планируется реализовать одну унифицированную модель, которая сможет реализовывать быстрое выявление максимально возможного количества различных видов угроз безопасности на уровне устройства. Идеальным узлом для работы такой модели представляются встраиваемые системы.  ***План исследования и план работы по диссертации.***  Планирование по ВКР было реализовано в двух основных направлениях: план исследования и план работы по диссертации, который помимо научно-исследовательских задач охватывает учебные, организационные и технические вопросы.  В максимально сжатой форме план работы по диссертации выглядит следующим образом (с отметками о выполнении):  **На 2-й семестр**   |  |  |  |  | | --- | --- | --- | --- | | № | Мероприятие | сроки | Отметки | |  | Знакомство с информацией по научным руководителям и предложенным темам. | До 20.01.23 | Исп. | |  | Утверждение темы научного исследования | До 20.02.23 | Исп. | |  | Постановка цели и задач на исследование, гипотезы на исследование. | До 20.02.23 | Исп. | |  | Подготовка обзора источников и исследование практик по проблеме. | До 15.05.23 | Исп. | |  | Определение метода исследования проблемы (согласуется с руководителем). | До 15.05.23 | Исп. | |  | Сбор необходимых данных для исследования |  | Рано | |  | Написание введения и одной главы диссертации по обзору литературы. | До 15.05.23 | черновик | |  | Дополнительное обучение по программированию встраиваемых систем (2 программы на базе Coursera) | До 30.06.23 | Исп. | |  | Дополнительное обучение по электротехнике, программированию на ARDUINO, IoT (3 курса на платформе Stepik) | До 30.06.23 | Пройден 1 курс |   **На 3-й семестр**   |  |  |  |  | | --- | --- | --- | --- | | № | Мероприятие | сроки | Отметки | |  | Актуализация этапов работы и задач по исследованию, данных и т. п. |  |  | |  | Сбор необходимых данных для исследования |  |  | |  | Проведение практической части исследования (эксперимент, тестирование модели, обучение нейросети и другое). |  |  | |  | Написание теоретического блока текста главы о выбранном методе, проведении тестирований и выводов по ней. |  |  | |  | Оформление прототипа модели |  |  |   **На 4-й семестр**   |  |  |  |  | | --- | --- | --- | --- | | № | Мероприятие | сроки | Отметки | |  | Доработка предыдущих глав. |  |  | |  | Уточнение практики, доработка, повторное тестирование. |  |  | |  | Анализ и выводы по исследованию |  |  | |  | Написание финальных разделов главы и заключения |  |  | |  | Редактура диссертации (финальный вид по ГОСТам). |  |  | |  | Защита ВКР |  |  |   Рабочий план исследования структурирован следующим образом:  **Введение**  **1. Использование нейронных сетей в решении задач обеспечения безопасности встраиваемых систем, реализующих технологии CV. Обзор проблемы и литературы**  1.1. Функционирование Интернета вещей. Современные подходы, модели и технологии  1.2. Моделирование угроз безопасности на уровне встраиваемых систем и основные методы их обнаружения, блокирования и устранения  1.3 Ключевые особенности использования алгоритмов машинного обучения, экспертных систем и условных конструкций во встраиваемых системах для устройств, реализующих технологии CV.  1.3. Конкуренция статистических методов, моделей классического машинного обучения и нейронных сетей в задачах обнаружения аномалий  1.4 Иные методы детектирования угроз безопасности  **2. Адаптация моделей глубоких нейронных сетей для решения задач обеспечения безопасности на уровне встраиваемых систем**  2.1. Теоретическое обоснование выбора архитектуры модели и ее проектирование  2.2. Исходные данные и их предварительная обработка  2.3 Метод оценки, метрики и системы тестирования  2.4. Использование основного функционального CV алгоритма, для обеспечения безопасности встраиваемой системы  **3. Реализация алгоритма. Тестирование, настройка и результаты**  3.1 Тестирование модели на стандартных наборах и специально подготовленных данных  3.2 Тестирование модели на платформах, имитирующих угрозы безопасности  3.3. Оценка результатов, выводы и дальнейшие перспективы  **Заключение**  **Список использованной литературы**  ***Источники исследования. Ниже приведены изученные наиболее цитируемые статьи по рассматриваемой проблематике за последние 4 года и более ранние, но значимые исследования:***   1. Tariqa N., Khan F.A., Asimc M. Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis // Procedia Computer Science. 2021. Vol. 191. PP. 425‒430. DOI: 10.1016/j.procs.2021.07.053 2. Sengupta J., Ruj S., Das Bit S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT // Journal of Network and Computer Applications. 2019. Vol. 149. DOI: 10.1016/j.jnca.2019.102481 3. Муренин И.Н. Обнаружение аномалий в трафике устройств Интернета вещей // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 128‒137. DOI:10.31854/1813-324X-2021-7-4-128-137 4. Enoch S.Y., Ge M., Hong J.B., Kim D.S. Model-based Cybersecurity Analysis: Past Work and Future Directions. Cornell University, 2021. URL: https://arxiv.org/abs/2105.08459 (дата обращения 21.12.2021) 5. Torres N., Pinto P., Lopes S.I. Security Vulnerabilities in LPWANs ‒ An Attack Vector Analysis for the IoT Ecosystem // Applied Sciences. 2021. Vol. 11. Iss. 6. DOI:10.3390/app11073176 7. Alansari Z., Anuar N.B., Kamsin A., Belgaum M.R., Alshaer J., Soomro S., et al. Internet of Things: Infrastructure, Architecture, Security and Privacy // Proceedings of the International Conference on Computing, Electronics & Communications Engineering (iCCECE, Southend, UK, 6‒17 August 2018). IEEE, 2018. DOI:10.1109/iCCECOME.2018.8658516 7. Hamza A., Gharakheili H.H., Sivaraman V. IoT Network Security: Requirements, Threats, and Countermeasures. Cornell University, 2020. URL: https://arxiv.org/abs/2008.09339 (дата обращения 21.12.2021) 8. Bouazza H., Zohra L.F., Said B. Integration of Internet of Things and Social Network: Social IoT General Review // Proceedings of the First International Conference on Computing (ICC 2019, Riyadh, Saudi Arabia, 10–12 December 2019) on Advances in Data Science, Cyber Security and IT Applications. Communications in Computer and Information Science. Vol. 1098. Cham: Springer, 2019. PP. 312‒324. DOI:10.1007/978-3-030-36368-0\_26 9. Ali O., Ishak M.K., Bhatti M.K.L. Emerging IoT domains, current standings and open research challenges: a review // PeerJ Computer Science. 2021. DOI:10.7717/peerj-cs.659 10. Nguyen-An H., Silverston T., Yamazaki T., Miyoshi T. IoT Traffic: Modeling and Measurement Experiments // IoT. 2021. Vol 2(1). PP. 140‒162. DOI:10.3390/iot2010008 11. Charyyev B., Gunes M.H. Detecting Anomalous IoT Traffic Flow with Locality Sensitive Hashes // Proceedings of the Global Communications Conference (GLOBECOM, Taipei, Taiwan, 7‒11 December 2020). IEEE, 2020. DOI:10.1109/GLOBE COM42002.2020.9322559 12. Garlisi D., Martino A., Zouwayhed J., Pourrahim J., Cuomo F. Exploratory approach for network behavior clustering in LoRaWAN // Journal of Ambient Intelligence and Humanized Computing. 2021. DOI:10.1007/s12652-021-03121-z 13. Fu C., Zeng Q., Du X. HAWatcher: Semantics-Aware Anomaly Detection for Appified Smart Homes // Proceedings of the 30th USENIX Security Symposium (USENIX Security 21). USENIX Association, 2021. PP. 4223‒4240. URL: https://www.usenix.org/conference/usenixsecurity21/presentation/fu-chenglong 14. Bhatia R., Benno S., Esteban J., Lakshman T.V., Grogan J. Unsupervised machine learning for network-centric anomaly detection in IoT // Proceedings of the 3rd ACM CoNEXT Workshop on Big Data, Machine Learning and Artificial Intelligence for Data Communication Networks (Big-DAMA '19). New York: Association for Computing Machinery, 2019. PP. 42‒28. doi:10.1145/3359992.3366641 15. Nõmm S., Bahşi H. Unsupervised Anomaly Based Botnet Detection in IoT Networks // Proceedings of the 17th International Conference on Machine Learning and Applications (ICMLA, Orlando, USA, 17‒20 December 2018). IEEE, 2018. DOI:10.1109/ICMLA.2018.00171 16. Alrawais A., Alhothaily A., Hu C., Cheng X. Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing, 2017, no. 21(2), pp. 34–42. doi:10.1109/MIC.2017.37 2. 17. Браницкий А. А., Котенко И. В. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейро-нечетких классификаторов. Информационно-управляющие системы, 2015, № 4, с. 69–77. doi:10.15217/issn1684-8853.2015.4.69 18. Гайфулина Д. А., Котенко И. В. Применение методов глубокого обучения для решения задач кибербезопасности. Ч. 1. Вопросы кибербезопасности, 2020, № 3(37), с. 76–86. doi:10.21681/2311-3456- 2020-03-76-86 19. Гайфулина Д. А., Котенко И. В. Применение методов глубокого обучения для решения задач кибербезопасности. Ч. 2. Вопросы кибербезопасности, 2020, № 4(38), с. 11–21. doi:10.21681/2311-3456- 2020-04-11-21 20. Al-Garadi M. A., Mohamed A., Al-Ali A., Du X., Guizani M. A Survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 2020, vol. 22, no. 3, pp. 1646–1685. doi:10.1109/COMST.2020.2988293 21. Левшун Д. С., Гайфулина Д. А., Чечулин А. А., Котенко И. В. Проблемные вопросы информационной безопасности киберфизических систем. Информатика и автоматизация, 2020, т. 19, № 5, с. 1050– 1088. doi:10.15622/ia.2020.19.5.6 22. HaddadPajouh H., Dehghantanha A., Khayami R., Choo K. K. R. A Deep recurrent neural network based approach for internet of things malware threat hunting. Future Generation Computer Systems, 2018, vol. 85, pp. 88–96. doi:10.1016/j.future.2018.03.007 23. Muna Al H., Moustafa N., Sitnikova E. Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications, 2018, vol. 41, pp. 1–11. doi:10.1016/j.jisa.2018.05.002 24. Alom M. Z., Bontupalli V., Taha T. M. Intrusion detection using deep belief networks. 2015 National Aerospace and Electronics Conference (NAECON), Dayton, 2015, pp. 339–344. doi:10.1109/NAECON.2015. 7443094 25. Yin C., Zhu Y., Fei J., He X. A Deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 2017, vol. 5, pp. 21954–21961. doi:10.1109/ACCESS.2017.2762418 26. Tang T. A., Mhamdi L., McLernon D., Zaidi S., Ghogho M. Deep learning approach for network intrusion detection in software defined networking. 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), 2016, pp. 258–263. doi:10.1109/WINCOM.2016.7777224 27. Ludwig S. A. Intrusion detection of multiple attack classes using a deep neural net ensemble. 2017 IEEE Symposium Series on Computational Intelligence (SSCI), Honolulu, 2017, pp. 1–7. doi:10.1109/SSCI. 2017.8280825. 28. Parra G. D. L. T., Rad P., Choo K. K. R., Beebe N. Detecting internet of things attacks using distributed deep learning. Journal of Network and Computer Applications, 2020, vol. 163, pp. 102662. doi:10.1016/ j.jnca.2020.102662 29. Roopak M., Tian G. Y., Chambers J. Deep learning models for cyber security in IoT networks. 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, USA, 2019, pp. 0452–0457. doi:10.1109/CCWC.2019.8666588 30. Cui J., Long J., Min E., Liu Q., Li Q. Comparative study of CNN and RNN for deep learning-based intrusion detection system. International Conference on Cloud Computing and Security, Springer, Cham, 2018, pp. 159–170. doi:10.1007/978-3-030-00018-9\_15 31. Nwankpa C., Ijomah W., Gachagan A., Marshall S. Activation functions: Comparison of trends in practice and research for deep learning. ArXiv preprint arXiv:1811.03378, 2018. 20 p. 32. Srivastava N., Hinton G., Krizhevsky A., Sutskever I., Salakhutdino R. Dropout: a simple way to prevent neural networks from overfitting. The Journal of Machine Learning Research, 2014, vol. 15, no. 1, pp. 1929–1958. 18. UNSW-NB15 Dataset. https://www.unsw.adfa.edu. au/unsw-canberra-cyber/cybersecurity/ADFANB15-Datasets/ (дата обращения: 27.10.2020). 33. Moustafa N., Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, 2015, pp. 1–6. doi:10.1109/ MilCIS.2015.7348942 34. Moustafa N., Turnbull B., Choo K. R. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. IEEE Internet of Things Journal, 2019, vol. 6, no. 3, pp. 4815–4830. doi:10.1109/ JIOT.2018.2871719   ***Выбранные методы исследования (с пояснением и аргументацией вашего выбора)***  С учетом задач, изложенных в тексте отчета в работе, наиболее активно будут использоваться следующие методы: анализ и синтез для извлечения, теоретического обобщения. Ключевыми методами в работе выбраны моделирование и эксперимент. Моделирование позволить масштабировать проблему, уточнить характер связей между объектами и представить целостную систему функционирования мира интернета вещей. Далее это позволит определить связи устройств, их функционал, используемые виды данных, технологические особенности объектов и т. д. Вся эта информация ляжет в основу другой модели – модели угроз, включающую их источники и методы воздействия. Суммарно эти модели станут методологической основой для разработки нейронной сети, способной эффективно выявлять и наибольшее количество угроз. (в перспективе планируется и написание протоколов защиты и программного кода, который будет эти протоколы запускать и блокировать угрозы)  Состоятельность гипотезы и собственно эффективность алгоритма будет проверятся путем проведения экспериментов – тестирования, реализовывать которое планируется в два этапа: 1) на популярных наборах данных, моделирующих угрозы безопасности IoT устройств; 2) на тестовых сервисах. Промежуточные результаты тестирования будут использоваться для доработки модели и настройки параметров |
| **Итоги НИР за семестр** | Участие в хакатонах, дататонах, чемпионатах по тематике проекта  (название, даты проведения, формат участия, сертификаты/победы) | *Участие в качестве капитана команды Excellent’s в хакатоне МФТИ и Skillfactory «Лаборатория решения реальных кейсов» с \_\_\_ по \_\_\_\_\_ (первое место в решении кейса от компании «работа.ру»).* |
| Участие в конкурсах на лучшую НИР и выставках (авторы, название работы и конкурса (экспоната и выставки)) | Не участвовал |
| Доклады на научных конференциях, семинарах (авторы, название доклада и конференции, место проведения) | Не участвовал |
| Научные публикации (авторы, название работы и издания) | нет |
| Медали, дипломы, грамоты, премии и т.п. на конкурсах на лучшую НИР и на выставках (авторы, название работы и конкурса (экспоната и выставки), вид награды) | нет |
| Проекты, поданные на конкурсы грантов (авторы, название и вид гранта) | нет |
| Полученные гранты (авторы, название и вид гранта) | нет |
|  | Другое (заявки и охранные документы на объекты интеллектуальной собственности, проданные лицензии на их использование, участие в инвест-сессиях и питчинг-сессиях, стипендии Президента и Правительства РФ и т.п.) | нет |
| **Материальная поддержка НИР студента за семестр (с указанием источника финансирования)** | | нет |
| **План работы на следующий семестр** | | **На 3-й семестр**   |  |  |  |  | | --- | --- | --- | --- | | № | Мероприятие | сроки | Отметки | |  | Актуализация этапов работы и задач по исследованию, данных и т. п. |  |  | |  | Сбор необходимых данных для исследования |  |  | |  | Проведение практической части исследования (эксперимент, тестирование модели, обучение нейросети и другое). |  |  | |  | Написание теоретического блока текста главы о выбранном методе, проведении тестирований и выводов по ней. |  |  | |  | Оформление прототипа модели |  |  | |
| **Отзыв научного руководителя** | | В рамках подготовки к написанию ВКР Самойлов Павел Александрович провел исследование литературы по теме проекта, определена структура и план исследования, Самойлов Павел Александрович успешно окончил несколько курсов по теме исследования, успешно принял участие в хакатоне по тематике, близкой по направленности к теме ВКР. |
| **Оценка НИР студента за семестр** | | **10** |

**Студент Самойлов Павел Александрович**  **дата составления отчета 12.05.2023\_\_\_\_**

**Научный руководитель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_Глинский А.В.\_\_\_\_\_/**

**Зав. Кафедрой\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/**