**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |
| --- | --- |
|  | **ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ**  **Кафедра**  **«Криптология и кибербезопасность»** |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Отчет**

**о научно-исследовательской работе**

«Обнаружение внутреннего нарушителя путём выявления стрессового состояния пользователя на основе анализа взаимодействия с клавиатурой и мышью с применением алгоритмов машинного обучения»

|  |  |  |
| --- | --- | --- |
| Исполнитель:  студент гр. Б16-506 | \_\_\_\_\_\_\_\_\_\_\_ (подпись, дата) | Султанов А.Э. |
| Научный руководитель: | \_\_\_\_\_\_\_\_\_\_\_ (подпись, дата) | Когос К.Г. |
| Зам. зав. каф. № 42: | \_\_\_\_\_\_\_\_\_\_\_ (подпись, дата) | Когос К.Г. |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Москва – 2019**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**РЕФЕРАТ**

СОДЕРЖАНИЕ

**ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

# 

# ВВЕДЕНИЕ

В современном мире информационных технологий обеспечение информационной безопасности становится всё более сложной задачей. Несмотря на огромные усилия со стороны компаний, разрабатывающих средства эффективного противодействия информационным угрозам, для некоторых из угроз данная задача остаётся всё ещё нерешённой.

Одной из таких угроз, с которой сталкиваются большинство компаний, в той или иной степени связанных с миром технологий, является угроза внутреннего нарушителя. Данный вид угрозы представляет наибольшую опасность в силу огромного числа порождающих её источников и недостатка эффективных средств противодействия этой угрозе, вследствие чего компании несут огромные финансовые потери. Именно поэтому угроза внутреннего нарушителя является актуальной и на данный момент ей уделяется значительное внимание со стороны исследователей в мире информационной безопасности.

Объяснением отсутствия достаточного количества средств борьбы против угрозы внутреннего нарушителя является характер данной угрозы. Несмотря на то, что результат действий внутреннего нарушителя очевиден, очень сложно найти информативные показатели, которые позволили бы обнаружить аномальное поведение пользователя информационной системы и отличить его от нормального. Для анализа поведения можно использовать данные электрокардиограммы (ЭКГ) или электроэнцефалограммы (ЭЭГ) [1,2], температуры тела [1,3], кровяного давления [3], движения глаз [4] и других биометрических показателей.

Однако способы получения большинства видов биометрических показателей являются инвазивными, то есть требуют использования специального и дорогостоящего оборудования в виде датчиков и камер, которые чаще всего находятся в непосредственном контакте с участником эксперимента в процессе накопления данных. Этот недостаток является причиной того, что методы, разработанные на основе инвазивных способов получения биометрических показателей, сложно применить на практике.

При этом существуют некоторые неинвазивные способы накопления данных для анализа поведения, которые основы на использовании доступных инструментов, например клавиатуры и мыши, которые легко можно найти в любом офисе. Эти недорогостоящие инструменты могут выступать в качестве датчиков, которые предоставляют поведенческую информацию или, иными словами, поведенческую характеристику, состоящую из клавиатурного почерка, динамики нажатия клавиш и жестов. Поведенческую характеристику можно использовать в решении задач аутентификации [5,6,7,8,9], детекции эмоционального состояния [10,11,12,13,14,15], а также в задачах обнаружения угрозы внутреннего нарушителя [16].

Данная работа посвящена исследованию методов обнаружения внутреннего нарушителя путём выявления стрессового состояния пользователя на основе анализа взаимодействия с клавиатурой и мышью. Как и в работе [16], исследование построено на проверке предположения о том, что при совершении неправомерных действий у внутреннего нарушителя под воздействием индуцированного стрессового состояния меняются поведенческие показатели. Однако в отличие от работы [16] применяется более обширный диапазон выделенных из сырых данных признаков и для подтверждения гипотезы используется большее число алгоритмов.

В первом разделе рассмотрен процесс накопления данных, включающий в себя требования к сценариям для накопления данных, их описание и обоснование использования данных сценариев.

Во втором разделе описан процесс выделения признаков из сырых данных, их обработка, а также рассмотрены модели классификаторов аномального и нормального поведения, построенные на основе различных алгоритмов машинного обучения.

В третьем разделе приведены результаты применённых моделей и проведена сравнительная характеристика этих моделей.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. **Abdulaziz A.** On the Possibility of Insider Threat Detection Using Physiological Signal Monitoring [Текст] / A. Abdulaziz, E. Khalil // Proc. of the ACM 7th International Conference on Security of Information and Networks — 2014.
2. **Hojae L.** An Application of Data Leakage Prevention System based on Biometrics Signals Recognition Technology [Текст] / L. Hojae, J. Junkwon, K. Taeyoung, P. Minwoo, E. Jungho, T.M. Chung // SUComS — 2013.
3. **Yessie H.** Inside the Mind of the Insider: Towards Insider Threat Detection Using Psychophysiological Signals [Текст] / H. Yessie, T. Hasan, G. Mohammad, D. Ram // Journal of Internet Services and Information Security — 2016.
4. **Hassan T.** Prediction of Human Error Using Eye Movements Patterns for Unintentional Insider Threat Detection [Текст] / T. Hassan, H. Yessir, D. Ram // IEEE 4th International Conference on Identity, Security, and Behavior Analysis — 2018.
5. **Bergadano F.** Identity verification through dynamic keystroke analysis [Текст] / F. Bergadano, D. Gunneti, C. Picardi // Intelligence Data Analisys Journal 7 — 2003.
6. **Dowland P.** A Long-term trial of keystroke profiling using digraph, trigraph and keyword latencies [Текст] / P. Dowland, S. Furnell // In IFIP International Federation for Information Processing Journal — 2004.
7. **Joyce R.** Identity authentication based on keystroke latencies [Текст] / R. Joyce, G. Gupta // Commun. ACM 33 — 1990.
8. **Monrose F.** Keystroke dynamics as a biometric for authentication [Текст] / F. Monrose, A. D. Rubin // Future Generation Computing Systems 16 — 2000.
9. **Bender S.** Key sequence rhythm recognition system and method [Текст] / Bender, S. and Postley, H // (U.S. Patent № 7 206 938) — 2002.
10. **Kołakowska A.** Recognizing emotions on the basis of keystroke dynamics [Текст] / A. Kołakowska // 2015 8th International Conference on Human System Interaction (HSI) — 2015.
11. **Epp C.** Identifying Emotional States using Keystroke Dynamics [Текст] / C. Epp, M. Lippold, R. L. Mandryk // Proceedings of the International Conference on Human Factors in Computing Systems — 2011.
12. **Nazmul Haque F.M.** Identifying Emotion by Keystroke Dynamics And Text Pattern Analysis [Текст] / F.M. Nazmul Haque, J.M. Alam // Behaviour and Information Technology Journal — 2012.
13. **Suranga D.W.G.** Non Invasive Human Stress Detection Using Key Stroke Dynamics and Pattern Variations [Текст] / D.W.G. Surang, M. De Silva Pasan, S.B.K. Dayan, M.K.D. Arunatileka Shiromi // International Conference on Advances in ICT for Emerging Regions (ICTer) — 2013.
14. **Kołakowska A.** Towards detecting programmers’ stress on the basis of keystroke dynamics [Текст] / A. Kołakowska // Proceedings of the Federated Conference on Computer Science and Information Systems — 2016.
15. **Ulinskas M.** Recognition of human daytime fatigue using keystroke data [Текст] / M. Ulinskasa, R. Damaševičiusa, R. Maskeliūnasa, M. Woźniak // The Workshop on Computational Intelligence in Ambient Assisted Living Systems (CIAALS 2018) — 2018.
16. **Yassir H.** Insider Threat Detection Based on Users’ Mouse Movements and Keystrokes Behavior / H. Yassir, T. Hassan, D. Ram // Conference Secure Knowledge Management Conference — 2017.