УДК 004.942

ИССЛЕДОВАНИЕ МОДЕЛИ ВЫЯВЛЕНИЯ ИНСАЙДЕРА С ПОМОЩЬЮ ПСИХОФИЗИОЛОГИЧЕСКОЙ ЭКСПЕРТИЗЫ НА ОСНОВЕ БИОМАРКЕРОВ.

Пенин А.С. (ФГАОУ ВО «Национальный исследовательский университет ИТМО)
Научный руководитель – декан факультета БИТ, к.т.н Заколдаев Д.А.
(ФГАОУ ВО «Национальный исследовательский университет ИТМО)
Научный консультант – доцент факультета БИТ, к.т.н Коржук В.М.
(ФГАОУ ВО «Национальный исследовательский университет ИТМО)

В ходе данной научной работы была разработана и исследована модель выявления инсайдеров с помощью психофизиологический экспертизы на основе биомаркеров. Был рассмотрен принцип действия модели, проведена оценка работы входящих в неё систем. По результатам анализа было принято решение о необходимости дальнейшего совершенствования полученной модели.

Введение. Безопасность информационных систем всё больше подвергается риску со стороны внутренних угроз. До 43% утечек данных компаний за 2020 год было вызвано инсайдерами, что на 34% больше, чем в 2019 году[1]. Растет при этом и средняя стоимость таких инцидентов.

Целью данной научно-исследовательской работы является исследования модели выявления инсайдера с помощью психофизиологической экспертизы на основе биомаркеров. Задачами научно-исследовательской работы являются разработка модели, её первичное исследование и анализ результатов исследования.

Предпосылкой к исследованию именно методики психофизиологической экспертизы была оценка методики как перспективной, но не способной в данный момент полностью раскрыть весь потенциал. Для того, чтобы понять причины этого и было принято решение о её изучении. Было выявлено основное достоинство этих методик - высокий потенциал к идентификации злоумышленников инсайдеров, отмеченный многими авторами[2][3] исследованных работ. Однако были обнаружены следующие общие недостатки:

- точность экспертизы варьирует в зависимости от частных биологических признаков;
- влияние навыков эксперта в интерпретации данных на результат экспертизы;
- необходимость дорогостоящего оборудования для снятия информации о состоянии испытуемого;
- влияние знания испытуемого о методиках проведения экспертизы на результат экспертизы;
- этический вопрос.

Был проведен поиск путей, которыми можно было бы компенсировать выявленные недостатки методики психофизиологической экспертизы, чтобы повысить её точность, надежность и снизить стоимость её проведения. Предложенным решением является использование носимых устройств для сбора информации о состоянии организма сотрудников и последующий её анализ с помощью моделей машинного обучения, для создания базы данных маркеров связи состояния организма каждого отдельного сотрудника с его психическим состоянием.

Таким образом был предложен следующий алгоритм работы модели. Носимое устройство в режиме онлайн собирает данные о состоянии сотрудника, затем эти данные передаются в систему оценки стресса и физической нагрузки. Эта система анализирует данные, с целью определить индивидуальные характеристики биомаркеров для различных уровней

стресса и активности. Затем эти данные заносятся в защищенную БД и закрепляются за сотрудником. После формирования банка данных может быть проведена психофизиологическая экспертиза, во время которой уровни реакций сотрудников также будут оцениваться и сравниваться с характерными для них. Выявление несоответствий при этом будет служить основанием для проверки деятельности сотрудника.

Было проведено первичное исследование компонентов модели: системы оценки физической нагрузки сотрудников, системы оценки стресса сотрудников, системы защищенного хранения данных Системы оценки показали первичную среднюю точность 75%, дальнейшие исследования будут направлены на её повышение. При этом достоверность результатов проведенной психофизиологической экспертизы повысилась на 35%.

Выводы. В ходе данное научно-исследовательской работы была разработана и протестирована модель выявления инсайдера с помощью психофизиологической экспертизы на основе биомаркеров. Первые испытания показали, что разработанные системы оценки физического состояния и стресса сотрудников в среднем демонстрируют точность в 75%, данный показатель необходимо будет повысить в ходе дальнейших исследований. При этом уже полученных результатов достаточно для того, чтобы повысить достоверность результатов проведенной психофизиологической экспертизы на 35%. Исследования в этом направлении будут продолжены.

Список использованных источников:

1. Widup S., Hylender D., Basset G.. Verizon Data Breach Investigation Report – 2020. – DOI:10.13140/RG.2.2.21300.48008
2. Yassir Hashem, Hassan Takabi, Mahhamad GhasemGol. Inside the Mind of the Insider: Towards Insider Threat Detection Using Psychophysiological Signals // Journal of Internet Services and Information Security. – 2016. – № 6. – С. 20–36
3. Yassir Hashem. Psychophysiological and Behavioral Measures Used to Detect Malicious Activities. // CyberSecurity for Information Professionals. – 2020 - 1

Пенин А.С.

Коржук В.М. (научный консультант)