УДК 004.942

ИССЛЕДОВАНИЕ ПСИХОФИЗИОЛОГИЧЕСКОЙ ЭКСПЕРТИЗЫ КАК МЕТОДИКИ ПРОТИВОДЕЙСТВИЯ ИНСАЙДЕРСКИМ АТАКАМ.

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 было проведено исследование различных методов противодействия атакам инсайдеров с помощью психофизиологический экспертизы. Были рассмотрены достоинства и недостатки таких методик. Было принято решение о разработке новой методики, которая могла бы обойти существующие недостатки.

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 психофизиологической экспертизы как методики противодействия инсайдерским атакам с целью выявления возможностей её модернизации. Задачами научно-исследовательской работы являются анализ источников и формирование предложений по модернизации методики на основе результатов анализа.

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.

В ходе выполнения научно-исследовательской работы были рассмотрены следующие методики психофизиологической экспертизы:

- полиграфическое тестирование;
- анализ движений глаз;
- анализ голоса;
- анализ мозговых волн;
- анализ поведенческой биометрии.

Достоинством этих методик можно считать высокий потенциал к идентификации злоумышленников инсайдеров, отмеченный многими авторами[2][3] исследованных работ

Их анализ позволил выявить 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. В дальнейшем будут проводиться дополнительные исследования в этом направлении.

Выводы. Выполненный в ходе данной научно-исследовательской работы анализ позволил выявить и систематизировать основные недостатки психофизиологической экспертизы как методики противодействия инсайдерским атакам. Основываясь на этих недостатках предлагается путь модернизации методики с использованием новейших технологий для раскрытия её потенциала. 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)