УДК 004.056.53

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ЗАЩИТЫ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ШИФРОВАНИЯ

Еремук В.В. (ИТМО), **Ромашов В.А.** (ИТМО), **Чернов Р.И.** (ИТМО)
Научный руководитель – д.т.н., доцент Гришенцев А.Ю.
(ИТМО**)**

Введение. В условиях растущей цифровизации различных отраслей экономики [1], вопрос обеспечения информационной безопасности становится всё более актуальным. Одним из ключевых направлений в рамках задачи обеспечения информационной безопасности является защита от вредносного программного обеспечения (ВПО) [2]. В последние годы значительно увеличилось количество киберпреступлений, связанных с применением программ-вымогателей (Ransomware) [3]. При заражении целевого устройства, вредоносное обеспечение, принадлежащее к данному типу, зашифровывает данные и требует выкуп за предоставление ключа [4]. Таким образом, защиту от данного типа ВПО можно построить на основе решения, обеспечивающего защиту данных от несанкционированного шифрования. Задачами данной работы являются:

1. разработка механизма отслеживания файловых операций на уровне ядра операционной системы;
2. выявление признаков, характерных для файловых операций, выполняемых при использовании алгоритмов шифрования;
3. разработка защищенного файлового хранилища;
4. разработка механизма для защиты данных от несанкцинированного шифрования на основе признаков, выявленных в пункте 2, и политик, основанных на принципе «белого списка»;

Целью данного исследования является разработка программных методов и средств защиты электронных документов от несанкционированного шифрования.

Основная часть.

В рамках исследования предложен механизм отслеживания файловых операций на уровне ядра операционных систем семества Windows. Разработано защищенное файловое хранилище. Также, в рамках исследования проанализированы файловые операции, выполняемые над файлами форматов .docx, .xlsx, .pptx при зашифровании файлов данных форматов посредством алгоритма AES. Указанные форматы основаны на формате ZIP-архивов [5]. В результате анализа обнаружены следующие признаки применения алгоритмов шифрования:

1. увеличение энтропии файлов, входящих в архив;
2. нарушение сигнатуры формата;

На основе выявленных признаков разработан механизм, выполняющий резервное копирование файлов в защищенное хранилище при обнаружении выполнения алгоритмов шифрования программным обеспечением, не находящимся в «белом списке». Также, в рамках исследования предложены подходы по формированию «белого списка» программного обеспечения, для которого выполнение зашифрования электронных документов является допустимой операцией.

Выводы. В результате исследования разработано программное средство для предотвращения несанкционированного шифрования электронных документов, позволяющее обеспечить защиту устройств от вредоносного программного обеспечения типа Ransomware. Предложены подходы по адаптации разработанного программного средства для других операционных систем.

Список использованных источников:

1. Куликова Г. А. Развитие цифровизации российской экономики //Актуальные вопросы экономики и агробизнеса. – 2019. – С. 136-141.
2. Семеко Г. В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия //Социальные новации и социальные науки. – 2020. – №. 1 (1). – С. 77-96.
3. Razaulla S. et al. The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions //IEEE Access. – 2023.
4. Meurs T. et al. Ransomware economics: a two-step approach to model ransom paid //18th Symposium on Electronic Crime Research, eCrime 2023. – 2023.
5. Sergeev A. V., Khorev P. B. Overview on hiding data in microsoft office documents //2021 3rd International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE). – IEEE, 2021. – С. 1-4.