ВВЕДЕНИЕ

Количество хранимой и обрабатываемой информации растет с каждым днем [23]. И для расследования правонарушений (инцидентов) связанных со средствами вычислительной техники и внутреннего аудита их содержимого, рост объемов данных является проблемой. Одним из возможных решений является классификация данных, которые относятся непосредственно к операционной системе и деятельности пользователя. Это позволит снизить объемы обрабатываемой информации экспертам, исследуя только те данные, которые относятся к деятельности пользователя и инцидентам. Таким образом возникает потребность в методах классификации пользовательских и системных данных на основе атрибутов в средствах вычислительной техники.

Как известно, у файлов, хранящихся на носителе информации имеются различные атрибуты, которые могут так или иначе относиться или к пользовательским или к системным. Определив информативность каждого из признаков, можно классифицировать файлы с носителя информации по атрибутам на пользовательские и системные.

Целью данной выпускной квалификационной работы является разработка методики классификации пользовательских и системных данных в средствах вычислительной техники на основе атрибутов. Для достижения поставленной цели была сформирована выборка данных, в дальнейшем из нее был выделен набор определенных атрибутов, путем оценки их информативности и важности для идентификации и расследования инцидента ИБ.

Для реализации поставленной цели было поставлено несколько задач. Во-первых, подготовка экспериментальных данных. Для этого составляются выборки данных с разных состояний работы операционной системы. Во-вторых, выбор средств получения и анализа данных. В-третьих, выбор

алгоритмов классификации. В-четвертых, получение результатов на экспериментальных данных.

В главе 1 рассматриваются теоретические основы и производится обзор существующей литературы, затрагивающей данную проблематику.

В главе 2 описываются предложенные решения поставленных задач из главы 1 и подробно рассматривается методика классификации пользовательских и системных данных.

В главе 3 приводится описание практического эксперимента и результаты работы разработанной методики. Производится сравнительный анализ методов для выявления лучших показателей точности.

ЗАКЛЮЧЕНИЕ

Методика классификации пользовательских и системных данных на основе атрибутов показала свою применимость в задачах проведения внутреннего аудита средств вычислительной техники. Ее использование позволяет определить информативность признаков, и на их основе рассчитать точность классификации данных на пользовательские и системные.

Был проведен эксперимент с применением предложенной методики, в ходе которого была рассчитана информативность и выделены наиболее значимые атрибуты. Полученные результаты могут быть использованы для расследования различных инцидентов информационной безопасности и анализа содержимого накопителя данных устройства.

Представленная методика не является конечным вариантом. В продолжение работы намечены следующие цели: разработка алгоритма учитывающего зависимость параметров (атрибутов) друг от друга и усовершенствование методики классификации файлов на системные и пользовательские.

Результаты эксперимента свидетельствуют о том, что данная методика имеет потенциал в развитии, и может применяться не только в задачах классификации пользовательских и системных данных при проведении внутреннего аудита, но и в других задачах компьютерной криминалистики.