Отзыв

на бакалаврскую работу Валейко Михаила Сергеевича

Модуль анализа поведения пользователей в SIEM-системах с целью выявления вредоносного ПО

Выпускная работа Валейко М.С. посвящена созданию модуля анализа поведения пользователей с целью выявления вредоносного ПО. В информационной безопасности анализ поведения пользователей используется для обнаружения внутренних угроз или вредоносных атак, целью которых является причинение вреда или получение несанкционированного доступа к внутренним ресурсам. Обнаружение и дальнейшее предотвращение таких атак является непростой и актуальной на сегодня задачей информационной безопасности. SIEM-системы обеспечивают анализ в реальном времени событий, исходящих от сетевых устройств и приложений.

По техническим причинам для создания модуля автор был ограничен использованием языка Python и пакета машинного обучения scikit-learn. В процессе работы над модулем автор столкнулся с рядом трудностей, которые он преодолел весьма успешно. Так, например, исходные данные оказались не размечены и, следовательно, это обстоятельство лишало возможности автора в случае реализации любого алгоритма оценить его эффективность. Для преодоления этой проблемы автор нашел размеченный dataset похожей структуры и именно его использовал для сравнительного анализа возможных алгоритмов из пакета scikit-learn. Кроме того, исходные данные оказались недостаточно информативны, но и это обстоятельство не остановило автора, и он нашел способ, позволяющий обогатить исходные данные (не искажая их содержание) с помощью открытой внешней системы VirusTotal. В дальнейших планах автора рассматривается внедрение реализованного модуля в промышленную эксплуатацию.

Своей работой автор продемонстрировал, что он в достаточной мере креативен, умеет работать с российскими и зарубежными источниками информации, владеет методами программирования и знаком с математическими приемами обработки и анализа данных. К недостатком работы можно отнести то, что автор слишком поздно выполнил работу и не довел ее до промышленной эксплуатации.

Указанные недостатки, тем не менее, не слишком снижают достоинства работы. Полагаю, что работа Валейко М.С. может быть оценена на “отлично”.

Научный руководитель

канд. физ-мат наук,

доцент Графеева Н.Г.