УДК 004.02

РАЗРАБОТКА СПОСОБА ИДЕНТИФИКАЦИИ ELF-ФАЙЛОВ НА ОСНОВЕ КЛАССИФИКАТОРА БАЙЕСА

Н.К. Мищенко, И.Е. Кривцова

Научный руководитель – Заколдаев Данил Анатольевич, к.т.н.

федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (Университет ИТМО), г. Санкт-Петербург

Одним из наиболее распространённых способов идентификации исполняемых файлов является идентификация, основанная на хэш-кодах. Также распространенным является способ идентификации с использованием электронной подписи. Так как оба способа имеют недостатки, разработка нового способа идентификация является актуальной. Идентификация по сигнатурам исполняемых файлов, основанных на дизассемблированном коде программы, сможет предотвратить возникновения новых уязвимостей автоматизированной системе, связанных с изменениями кода исполняемых файлов. Необходимость. На данный момент большинство существующих в области идентификации программ научных работ нацелено на обнаружение вредоносных программ. Комплексный подход к обеспечению информационной безопасности должен учитывать все возможные пути возникновения угроз. Данный метод нацелен на обнаружение изменений в коде исполняемых файлов, которые могут при выполнение нанести ущерб автоматизированной системе или повлечь за собой утечку данных.

Байесовский классификатор – это алгоритмы классификации, основанные на принципе максимума апостериорной вероятности. Наиболее распространенным в задачах информационной безопасности является наивный Байесовский классификатор. Данный классификатор является простым вероятностным классификатором, который применяет теорему Байеса, основываясь на строгих (наивных предположениях: каждый параметр классифицируемых данных рассматривается независимо от других параметров класса. Научную задачу можно сформулировать следующим образом: если в дизассемблированном коде есть какое-то изменение и отличие от эталона, то можно предположить, что данная программа нанесет ущерб автоматизированной системе.

Частные задачи:

- Исследование сигнатуры elf-файла.
- Сформирование схемы процесса идентификации.
- Поиск возможных модификаций классификатора Байеса для решения задач идентификации.
- Разработка алгоритма идентификации.
- Разработка метода идентификации elf-файлов на основе классификатора Байеса.
- Сравнение данного метода с существующими методами идентификации исполняемых файлов.
- Разработка наиболее эффективного метода. Сравнение созданного метода идентификации с существующими.
- Проведения тестирования метода.
- Анализ результатов.

Автор _____/ Мищенко Н.К.

Научный руководитель _____/ Заколдаев Д.А.

Декан ФБИТ _____/ Заколдаев Д.А.