Наименование ИТ-проекта
****
Межсетевой экран уровня веб-приложений Web application firewall

Перечень решаемых задач
****
1) Проксирование http-трафика к защищаемому веб-приложению
2) Фильтрация http-трафика путем его классификации на зловредный и легитимный с применением алгоритмов машинного обучения
3) Обучение системы с целью детектирования новых векторов распространенных классов атак на веб-приложения

Описание функциональных возможностей и элементов проекта
****
Состав программного обеспечения:
1) Консольный интерфейс для управления программным средством
2) Реализован как обратный прокси-сервер с возможностью фильтрации http-трафика
3) В качестве алгоритмов машинного обучения используются сторонние пакеты, разработанные на языке Python
4) Система включает в себя три модуля:
- обратный прокси-сервер
- модуль фильтрации трафика
- модуль машинного обучения

Дата внедрения
****
22.06.2018

Используемые платформы, средства разработки
****
Python, MongoDB, Visual Studio Code

Стоимость разработки системы
****
25000

Средний размер ежегодных затрат на эксплуатацию
****
7500

Перспективы развития
****
Разработка графического интерфейса для администрирования Web application firewall. Реализация других механизмов защиты, в т.ч. от DOS- и DDOS-атак

Новизна: отличие от аналогов или отсутствие аналогов
****
Большинство аналогов представляют защитные механизмы, основанные на машинном обучении, однако это сопровождается высокой ценой на данное ПО. В то же время, среди open-source представителей как правило механизмы машинного обучения для выявления вредоносного трафика отсутствуют

Завершенность проекта
****

Проект реализован, в процессе эксплуатации дополняется различными дополнительными функциями

Использование открытого кода (свободного ПО), отечественного программного обеспечения
****
Sklearn, numpy, MongoDB

Актуальность, экономическая или социальная полезность
****
Проблема безопасности веб-приложений является актуальной в связи постоянным появлением уязвимостей, а также новых векторов и видов атак

Масштабируемость, способность к взаимодействию с другими системами, мобильность
****
Программное средство является мобильным, благодаря этому может масштабироваться между территориально-удаленными филиалами организации