УДК 004.056

РАЗРАБОТКА МЕТОДА КЛАССИФИКАЦИИ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Хельштейн Э.В. (Университет ИТМО)
Научный руководитель – к.т.н., доцент Спивак А.И.
(Университет ИТМО)

Статья посвящена киберинцидентам и разработке метода классификации событий в сетевом трафике на основе анализа данных.

С увеличением масштабов компьютерных сетей наблюдается рост и количества информационных угроз и факторов, приводящих к нестабильному функционированию сетей передачи данных. Специалисты по всему миру постоянно ведут борьбу с киберпреступностью, и это вынуждает злоумышленников совершенствовать свои инструменты для взлома, а организации уметь защищаться от них. Когда при нарушении информационной безопасности предприятия происходит некий инцидент, то эта компания нередко терпит убытки, и к такой организации снижается доверие со стороны заказчиков и клиентов. Таким образом, возникает задача исследования одной из основных ветвей проникновения и воздействия на систему – сетевого трафика.

Основной целью метода будет являться создание классификатора, который на основе анализа сетевого трафика, и при применении методов машинного обучения, будет не просто выявлять угрозы, а заранее выделять события, по которым можно будет выделять предпосылки к атакам по сети. Исследование заключается в поиске и анализе взаимосвязей типов событий в сетевом трафике. В ходе работы будут проанализированы дампы сетевого трафика с выделением событий, применена тестовая выборка для машинного обучения модели. В конечном итоге, такой классификатор должен работать в автоматическом режиме.

Данный классификатор может быть применён в финансовых организациях, в частности, банках. В ходе научно-исследовательской части будут рассмотрены все основные методы машинного обучения, возможные сетевые атаки, анализ киберинцидентов, оценка результатов эксперимента.

Хельштейн Э.В. (автор) _____

Спивак А.И. (научный руководитель) _____