Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)
Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)

Модели противодействия кибератакам на основе методов машинного обучения

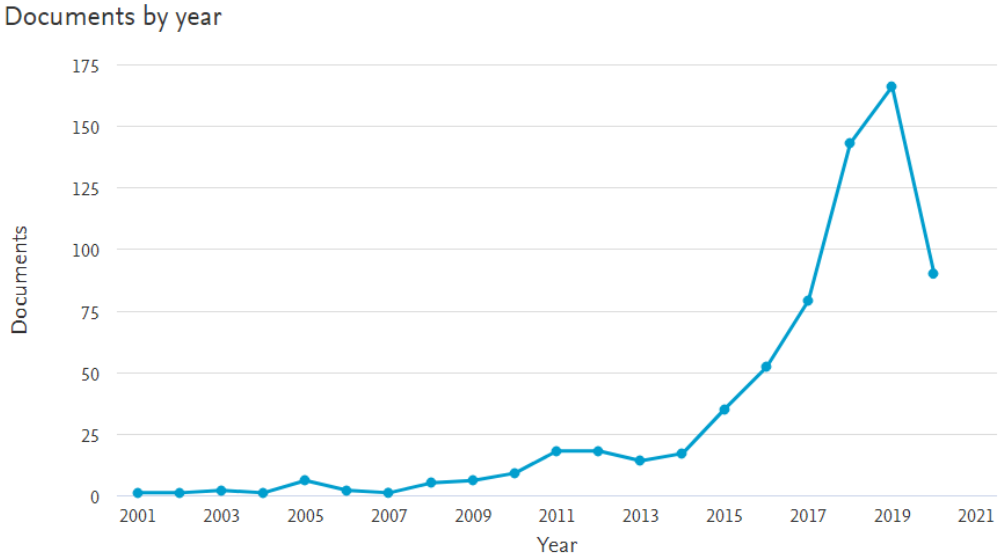
Перминов Петр Витальевич
аспирант 2 года обучения
ppv@fb.tusur.ru

Научный руководитель
Шелупанов Александр Александрович
д-р техн. наук, профессор

Томск 2020

Актуальность

- Несмотря на развитие средств защиты, ущерб от атак всё ещё огромен (по различным оценкам, до 2-3 трлн руб./год)
- Количество научных работ растёт
- Существуют требования регуляторов по обеспечению ИБ в КИИ, банковском секторе



Актуальность применительно к СОВ

- Существующие системы, как правило, генерируют большое количество ложных срабатываний
- Системы требуют тонкой настройки для различных инфраструктур
- В крупных инфраструктурах находится большое количество разнородных источников

Цели и задачи

Цель: повысить эффективность работы систем обнаружения инцидентов информационной безопасности путём снижения ошибок первого рода (ложноположительных срабатываний) и/или второго рода (пропуски инцидентов)

Задачи:

- Провести анализ подходов к построению моделей системы защиты информации и подходов к повышению кибербезопасности объектов
- Рассмотреть существующие решения
- Сбор и подготовка наборов данных (сетевого трафика, журналов действий пользователя в операционных системах), включающих информацию об атаках на защищаемую систему
- Разработать новую модель обнаружения инцидентов с использованием методов машинного обучения
- Программно реализовать данную модель
- Провести эксперимент и анализ результатов

Обзор публикаций

- Deep Learning Approach for Intelligent Intrusion Detection System,
  Vinayakumar R., Alazab M., Soman K.P., Poornachandran P., Al-Nemrat A.,Venkatraman S.
- Catch it if you can: Real-time network anomaly detection with low false alarm rates
  Kathareios G., Anghel, A., Mate, A., Clauberg, R., Gusat, M.
- Deep learning for prioritizing and responding to intrusion detection alerts
  McElwee S., Heaton J., Fraley J., Cannady, J. A user-centric machine learning framework for cyber security operations center
  Feng, C., Wu, S., Liu, N.

Deep Learning Approach for Intelligent Intrusion Detection System

- Область применения – системы обнаружения вторжений (IDS)
- Использовались глубокие нейронные сети
- Использовались следующие наборы данных для обучения и тестирования: KDDCup 99, NSL-KDD, UNSW-NB15, Kyoto, WSN-DS, CICIDS 2017
- Рассмотрены проблемы поиска и работы с тестовыми данными
- Точность распознавания – от 80% до 98%

Catch it if you can: Real-time network anomaly detection with low false alarm rates

- Анализ аномалий
- Уделено большое внимание проблеме ложных срабатываний
- 2х-этапное обучение: адаптивное автоматическое обнаружение аномалий и отсеивание ложных срабатываний с использованием классификатора на основе метода ближайших соседей
- Снижение уровня вмешательства человека снижено в 5 раз за счёт исключения ложных срабатываний
- Достигнута точность обнаружения в 98,5% при 1,5% ложных срабатываний

Deep learning for prioritizing and responding to intrusion detection alerts

- IDS
- Рассмотрена проблема ручного анализа сгенерированных инцидентов
- Предлагается методика классификации событий по важности FASST
- Формирование отчётов с индикацией компрометации системы (Indications of Compromise)

A user-centric machine learning framework for cyber security operations center

- Работа с SIEM + SOC
- Рассмотрена проблема ложноположительных срабатываний
- Продемонстрированы подходы к сбору и анализу данных, разработки функций и выбору подходящих алгоритмов
- Использовался метод опорных векторов для машинного обучения

Тестовые наборы данных

- KDD Cup 99
- NSL-KDD
- UNSW-NB15
- Kyoto
- WSN-DS
- CICIDS 2017

KDD Cup 99

- Недельный дамп сетевого трафика
- Содержит следующие маркированные атаки:
  - Отказ в обслуживании (DoS)
  - Повышение привелегий (U2R)
  - Удалённая атака (R2L)
  - Сбор информации (Probing Attack)
- Большое количество повторяющихся атак (около 75%)

NSL-KDD

- Выборка из KDD Cup 99
- Исключены нерелевантные записи из обучающего набора данных
- Изменено соотношение атак и легитимного трафика

UNSW-NB15

- Дамп трафика
- Значительно более современный относительно KDD Cup 99 (2015 против 1999 год)
- Более разнообразные и более современные атаки

Применимость методов и наборов данных для текущей задачи

- Существующие методы, как правило, протестированы на синтетических наборах, что не гарантирует эффективную работу на реальных
- Синтетические наборы данных представляют из себя сырые дампы трафика, что не подходит для SIEM-систем, однако они могут использоваться для сравнительной оценки различных алгоритмов и методов
- Для текущей задачи придётся создавать оригинальный набор данных

Что сделано

- Сданы кандидатские экзамены
- Публикация в Scopus
  Petr Perminov, Tatiana Kosachenko, Anton Konev, Alexander Shelupanov
  Automation of information security audit in the Information System on the example of a standard“ CIS Palo Alto 8 Firewall Benchmark” // International Journal of Advanced Trends in Computer Science and Engineering, Volume 9 No.2, March - April 2020
  https://doi.org/10.30534/ijatcse/2020/182922020
- Аналитический обзор в процессе
  Сейчас готово около 25 страниц, 30 источников
- Для подготовки наборов данных собраны события:
  - PT StandOff 2019
  - PT StandOff 2020
  - Легитимной активности на тестовой инфраструктуре

Модели противодействия кибератакам на основе методов машинного обучения

Перминов Петр Витальевич
аспирант 2 года обучения
ppv@fb.tusur.ru