**Титульник**

Здравствуйте, уважаемый председатель и члены аттестационной комиссии!

~4 секунд

**Актуальность темы**

Актуальность выбранной работы продиктована постоянным совершенствованием современных киберугроз, которые наносят значительный ущерб различным компаниям. Microsoft, Facebook, Acer, T-Mobile – это только основной список пострадавших, а перечисление можно продолжать долго.

И интеллектуальные системы посредством своего непрекращающегося мониторинга и выделения любых возникших отклонений выступают решением проблемы.

~21 секунд

**Цель и задачи работы**

Целью дипломной работы является – разработать систему для выявления аномалий сетевого трафика в виде модели искусственного интеллекта.

Для достижения этого необходимо было:

* Изучить влияние различных угроз на сетевой трафик.
* Провести анализ существующих методов обнаружения аномалий.
* Построить архитектуру системы и её программно реализовать.
* Сформировать набор входных данных для моделей.
* Проверить применимость методов искусственного интеллекта

~22 секунд

**Постановка задачи**

Решаемую задачу можно сформулировать так – имеется трафик реального предприятия, т. е. набор перехваченных сетевых пакетов. На основе него необходимо выучить поведения сетевых узлов – уметь их классифицировать с высокой точностью, что позволит детектировать аномалии в реальной работе при ошибочной классификации.

~17 секунд

**Распространённые причины аномалий**

В ходе анализа наиболее распространённых причин аномалий <пауза> сетевых угроз было заключено, что зачастую они выражаются в изменении интенсивности проходящего трафика (его повышение или понижение), направления трафика (по портам, сетевым узлам), увеличение или уменьшение числа потоков и т. д. И все это интеллектуальная система должна уметь качественно детектировать.

~19 секунд

**Существующие подходы в обнаружении аномалий**

По результатам анализа существующих подходов обнаружения аномалий были выделены следующие группы методов:

* Сигнатурные, основанные на применении регулярных выражений к наборам пакетов.
* Статистические, формирующие представление о нормальном и ненормальном трафике посредством различий в их статистических величинах.
* Методы искусственного интеллекта, которые представляются сейчас наиболее перспективными.
* Также теоретически возможная комбинация ранее описанных групп методов.

~23 секунд

**Выбранные модели ИИ**

В работе были выбраны следующие модели искусственного интеллекта:

* Случайный лес, который состоит из нескольких деревьев решений;
* Бустинг на решающих деревьях – где каждое следующее решающее дерево строится аддитивно для уменьшения ошибки предыдущего построенного дерева
* Многослойная искусственная нейронная сеть с прямой связью, архитектура которой представлена далее.

~20 секунд

**Архитектура нейронной сети**

Предложенная модель имеет:

* 3 слоя, выполняющих линейные преобразования;
* между которыми расположены функции активации ReLU, которые вычисляются как максимум от нуля и выхода предыдущего слоя;
* слои нормализации выходов слоёв – для стабильности обучения;
* слои Dropout, которые случайным образом отключает некоторые нейроны для решения проблемы переобучения;
* и последний слой это SoftMax, производящий нормализацию к вероятностям принадлежности к одному из классов.

~24 секунд

**Архитектура системы**

Центральная сущность работы — интеллектуальная система, архитектура которой представлена на слайде, она организована в набор модулей:

* Сперва *модуль захвата трафика* сохраняет весь трафик локальной сети и трафик Интернета, представляет в формат PCAP, хранящий набор его пакетов.
* Затем *модуль преобразования трафика* фильтрует данные и отбирает целостные, преобразует в формат сетевых соединений Netflow, который затем хранится в БД.
* После чего *модуль визуализации трафика* позволяет провести разведочный анализ имеющихся данных, а также составить графики поведения устройств.
* Далее *модуль подготовки данных* отбирает целевую выборку, вычисляет агрегационные простые параметры, производные параметры, делает балансировку обучающих выборок.

Далее данные передаются в *ядро системы обнаружения аномалий*, которое состоит из:

* *Модуля составления портрета*, отвечающего за отбор значимых признаков, обучение моделей, оптимизацию по их гиперпараметрам.
* И *модуля оценки* – конечного элемента системы, который применяет наилучшую модель в реальной работе.

~60 секунд

**Стек технологий**

Для программной реализации был выбран следующий стек технологий. Кроме наиболее распространённых библиотек Питона по машинному обучению и анализу данных, тут можно выделить:

* Imblearn – для балансировки обучающего набора данных.
* Plotly – для визуализации поведения сетевых узлов.
* СУБД Clickhouse – для хранения захваченного трафика в формате Netflow.
* А также утилиты TCPdump, Nfdump – для работы с трафиком в различных форматах.

~22 секунд

**Простые признаки сетевого трафика**

Здесь представлены простые признаки сетевого трафика. По сути, это формат Netflow в его первоначальном виде. Тут можно увидеть информацию о времени соединения, взаимодействующих узлах, интенсивности трафика и т. д. И зачастую только этих сведений недостаточно для принятия правильного решения, поскольку одно соединение довольно кратковременно.

Для устранения такой проблемы предлагается использовать новый подход, заключающийся в формировании агрегационных записей в историческом окне (обычно 10 минутный интервал), где будет считаться вся статистическая информация по представленным величинам.

Вдобавок к этим параметрам вычислялись и другие – производные.

~40 секунд

**Производные признаки сетевого трафика**

Которые представлены на данном слайде.

И всё это суммарно даёт набор входных данных, с которыми работают модели.

~10 секунд

**Исходный код проекта**

Здесь представлен QR код на репозиторий Github проекта.

~5 секунд

**Фрагмент используемого набора данных**

А тут представлен фрагмент используемого набора данных. Это перехваченный недельный сетевой трафик в формате Netflow.

~10 секунд

**Разведочный анализ данных**

Перед непосредственным обучением рассматриваемых моделей был проведён обязательный разведочный анализ сетевого трафика предприятия, т. е. обучающей выборки.

Имеются данные почти за трёхгодовой промежуток, в котором всего было обнаружено около полторы тысячи уникальных сетевых узлов.

На графиках видно, что данные о соединениях неравномерны – где-то наблюдались выбросы по соединениям и присутствует несбалансированность по числу записей каждого узла. Все это потребовало учёта при формировании обучающих выборок.

~25 секунд

**Поведение сетевых узлов**

На данном графике параллельных координат представлен пример статистики поведения некоторых узлов. Тут видно, как одна из рабочих машин ведёт себя почти схожим образом в разные дни – общее время активности, используемые порты, сервисы (т.е. порты получателя), но немного варьируется число потоков по сервису и число удалённых узлов взаимодействия.

~20 секунд

**Поведение сетевых узлов**

На следующем типе графиков отражена интенсивность сетевого трафика на различных устройствах по конкретным дням недели. Для рабочей станции здесь наблюдаются одинаковые периоды наивысшей активности, но разный объем трафика, тогда как для серверов показатель одинаковый.

Это указывает на то, что гипотеза о возможной разделимости узлов по информации об их потоках является довольно правдоподобной.

~21 секунд

**Результаты работы системы**

И что, собственно, в результате работы системы и было получено. Итак, здесь представлены итоги решения задачи выучивания поведения сетевых узлов – наилучшую точность показали модели градиентного бустинга XGBoost и нейронная сеть – около 90%.

Также была попытка обработки подмешенного вредоносного трафика в выборку с нормальным трафиком, и обе модели тут тоже в лидирующих позициях.

«Использовались средства генерации вредоносного трафика по типу Spirent CyberFlood, Metasploit, hping, BreakingPoint.»

~25 секунд

**Результаты работы**

Таким образом, разработана и успешно применена интеллектуальная система, которая качественным образом способна выучить поведение сетевых узлов и выявлять аномалии в их поведении.

Предложен новый подход в формализации входных данных сетевого трафика.

~15 секунд

**Отзывы**

Здесь представлены отзывы по проделанной работе – отзыв компании, где разрабатывалось решение и отзыв научного руководителя.

На этом у меня все. Спасибо за внимание

~10 секунд

Время в идеале: 6 минут 30 секунд.

Получается: 6 минут 26 секунд.