kaspersky

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ и БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

История, современность, перспективы

Сатанин Д.Н.

Немного [печальной] истории

- **1988 год: «Червь» Морриса**

2-го ноября Роберт Моррис, аспирант MIT, «протестировал» доступность узлов сети ARPANET («бабушку» сети Интернет). **ИТОГ**: заражено более **6 тысяч** узлов, потери – почти **100 млн** долларов и 3 года тюремного срока (условно).

- **2003 год: вирус Slammer (<u>всего 376 байт в оперативной памяти</u>)**

25 января за первые **10 минут** эпидемии заразил **75 тыс.** компьютеров. Отказы в работе серверного оборудования наблюдались практически по всему миру. В Южной Корее сеть Интернет не работала несколько часов.

- **2017 год: эпидемия WannaCry, exPetr etc**

Начало эпидемии: 12 мая, активная фаза – до начала июля. За **сутки** (12.05.2017 г.) было инфицировано более **130 тыс.** компьютеров в **99** странах. «Интернет-локдаун» на Украине – 27.06.2017 г.

Причины (и решение)

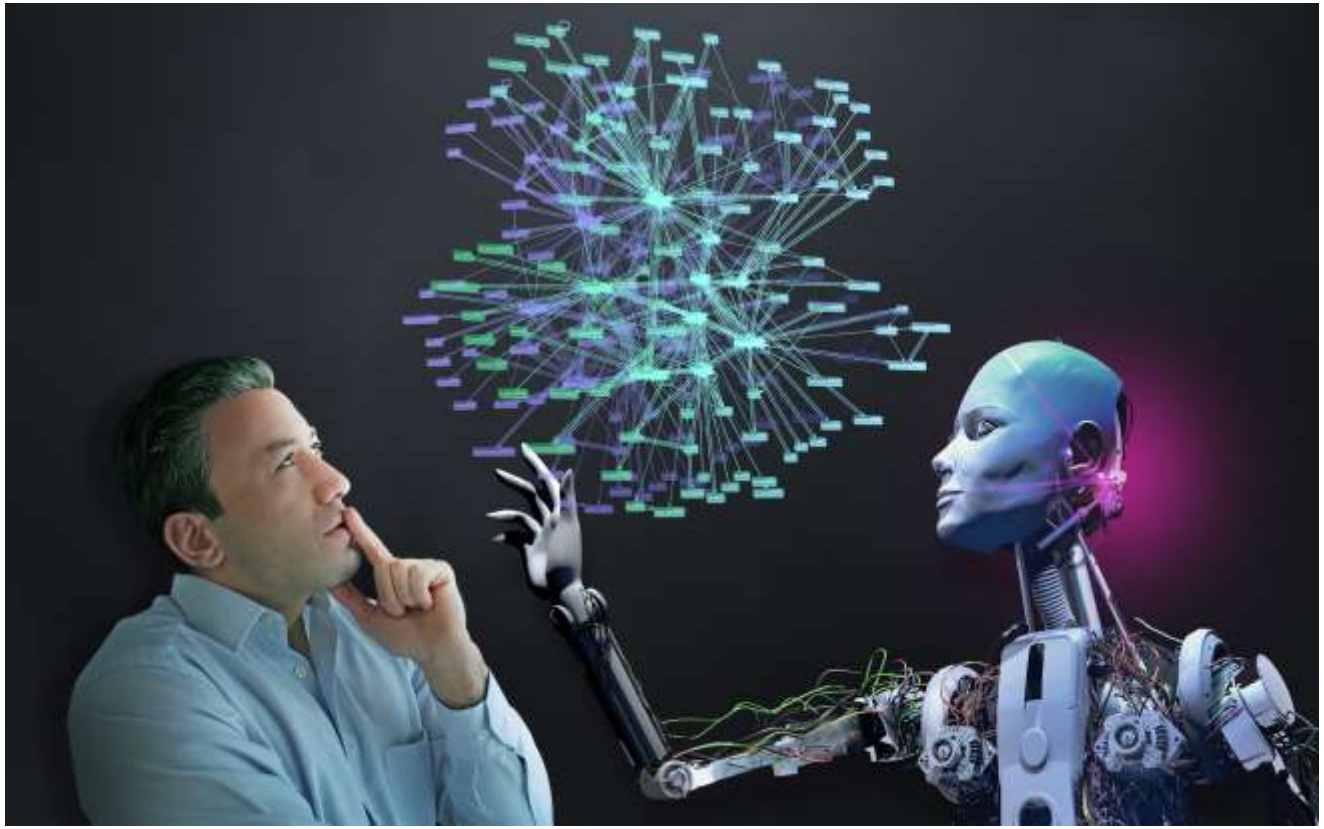
- Проблемы с БИ, которые высветил инцидент с «червём Морриса», носят системный (концептуальный) характер

- Предпринимаемых технических мер защиты явно недостаточно

- Необходим поиск, адаптация и апробация новых методов и подходов к обеспечению безопасности информации

Выход !!! (???)

- ✓ **Искусственный интеллект**



Ещё немного [интересной] истории (2002-2016 г.г.)

Задача: обнаружение компьютерных атак в сетевом трафике

- **многослойный персептрон (нейронная сеть прямого распространения, состоящая не менее, чем из трёх слоёв нейронов)**

МГУ им. Ломоносова, группа профессора Смелянского Р.Л.

- **алгоритмы, моделирующие пептиды (молекулы, формирующие иммунный ответ человека) или иммунные алгоритмы**

СПИИРАН (г. Санкт-Петербург), Лаборатория проблем компьютерной безопасности, под руководством Котенко И.В.

Практический эффект -

Причины (снова)

- **Высокая вычислительная сложность (и низкая производительность)**
- **Требовательность к вычислительным ресурсам**
- **Сильная зависимость от качества обучающей выборки и уровня подготовки эксперта**

Опыт «Лаборатории Касперского»

- **Контроль функционирования автоматизированных систем управления технологическими процессами (далее – АСУ ТП)**

- **Исследования цифровых артефактов (ЦА, в основном, файлов) на наличие элементов (признаков) неизвестного вредоносного ПО**

Опыт «Лаборатории Касперского» (продолжение)

Особенности АСУ ТП/ЦА:

- очень большое число сигналов (десятки тысяч)/различных ЦА
- высокая частота обновления сигналов (около 10 раз/сек)/ЦА (сотни/сек)
- длительное хранение «истории», всех зафиксированных значений/ЦА
- различные параметры одного ТП сильно взаимосвязаны его логикой и физическими законами/элементы ВПО достаточно «характерны»
- возможности внесения серьёзных искажений (в АСУ ТП)

Опыт «Лаборатории Касперского» (продолжение)

- **Контроль функционирования АСУ ТП - MLAD («Machine Learning for Anomaly Detection»):** позволяет зафиксировать признаки атаки на уровне технологических процессов и визуализирует это в терминах телеметрии, понятных оператору

Опыт «Лаборатории Касперского» (продолжение)

- Каждый ЦА был зафиксирован в соответствии с определённым набором параметров
- Сигнатурноым методом ЦА проверяется на принадлежность известному вредоносного ПО
- Если результат – отрицательный, то такой ЦАт поступает на вход ИИ-анализатора
- ИИ-анализатор «раскладывает» ЦА в две «корзины»: подозрительные на наличие вредоносного ПО и «чистые»
- «Чистые» ЦА помещаются в специальное хранилище и впоследствии могут быть повторно исследованы в случае необходимости
- Подозрительные ЦА подвергаются «ручной» обработке экспертом

Дообучение ИИ-анализатора происходит постоянно после идентификации ранее неизвестного вредоносного ПО

Опыт «Лаборатории Касперского» (обобщение)

«Секреты успеха»:

- большая и постоянно пополняемая коллекция образцов вредоносного ПО, что обеспечивает качественное начальное обучение
- регулярное дообучение
- квалифицированные эксперты
- значительные вычислительные мощности

Перспективы (светлые – ???)

Нынешние достижения в области ИИ:

- решение инженерных и программистских задач

Новые теоретические результаты:

- ???

Ключевая задача – развитие теории в области ИИ

- ***Необходимо серьёзно «вкладываться» в теоретические исследования***

kaspersky

СПАСИБО за ВНИМАНИЕ!

Вопросы?

- **АО "Лаборатория Касперского"**
- **Москва, 125212**
- **Ленинградское шоссе, д.39А, стр.3**
- **+7 (495) 797-87-00**
- **www.kaspersky.ru**