KASPERSKY lab

О КОМПАНИИ. О КУРСЕ. АКТУАЛЬНЫЕ КОМПЬЮТЕРНЫЕ УГРОЗЫ.

Александр Павлов

Руководитель группы подготовки и проведения тренингов

https://academy.kaspersky.ru/ ; https://securelist.ru/

ТЕМЫ КУРСА

Тема 1. Введение

- Примеры алгоритмов.
- Границы рационального познания.
- Сотрудничество человека и машины.

Тема 2. Анализ алгоритмов. Задачи сортировки

- Вычислимые функции. Рекурсивные функции.
- Временная и пространственная сложность алгоритмов. Классы P, PSPACE, NP.
- Классические вычислительные схемы. Дизъюнктивная нормальная форма. Обратимые вентили.
- Задачи сортировки: сортировка вставками, сортировка выбором, рекурсивная сортировка слиянием, рандомизированная сортировка.
- Двоичный поиск.

Тема 3. Рекурсивные алгоритмы

- Теорема об оценке сложности рекурсивного алгоритма.
- Рекурсивное умножение матриц методом Штрассена.
- Быстрое преобразование Фурье. Рекурсивное умножение многочленов.

- Решение задачи интерполяции с помощью интерполяционного многочлена Лагранжа и методом быстрого преобразования Фурье.

Темы 4-5. Алгоритмы на графах

- Практические задачи на теорию графов.
- Алгоритмы выхода из лабиринта.
- Представление графа матрицей смежности и списками смежности.
- Обход графа в глубину и его применения.
- Обход графа в ширину.
- Поиск кратчайшего пути в графе (алгоритм Дейкстры).
- Поиск критического (максимального) пути в графе.
- Покрывающие деревья: пример жадного алгоритма.
- Реализация алгоритма Крускала.

Темы 6-8. Числовые и криптографические алгоритмы

- Алгоритмы сложения, вычитания, умножения столбиком, рекурсивного умножения, деления.
- Мультипликативные функции. Теория сравнений. Теорема Эйлера. Распределение простых чисел.
- Арифметика сравнений: алгоритмы сложения, умножения и возведения в степень по модулю. Расширенный алгоритм Евклида, деление по модулю.
- Проверка чисел на простоту: тест Ферма.
- Генерация простых чисел.
- Протокол шифрования с одноразовым ключом. Стандарт AES.
- Протокол шифрования с открытым ключом. Алгоритм RSA.

Тема 9. Динамическое программирование

- Вычисление биномиальных коэффициентов.
- Кратчайшие пути в ориентированных ациклических графах.
- Поиск наибольшей строго возрастающей подпоследовательности.
- Оптимальная расстановка скобок при вычислении произведения не менее трех матриц.
- Оптимальная триангуляция многоугольника.
- Задача линейного разбиения.

Тема 10. Линейное программирование

- Примеры задач линейного программирования: оптимизация прибыли, транспортная задача.
- Задача о максимальном потоке в сетях.
- Простейшие матричные игры. Принцип минимакса.
- Симплекс-метод.

Тема 11. Квантовые алгоритмы

- Постулаты квантовой механики. Принцип неопределенности Гайзенберга.
  - Кубит. Система из двух кубитов.
  - Квантовые схемы.
  - Периодичность и квантовое преобразование Фурье.
  - Квантовый алгоритм разложения на множители.

Тема 12. Некоммутативная криптография

СПИСОК ЛИТЕРАТУРЫ

1. В.И.Игошин «Теория алгоритмов». 2013.
2. Стивен Скиена «Алгоритмы. Руководство по разработке». 2014.
3. С. Дасгупта, Х. Пападимитриу, У. Вазирани «Алгоритмы». 2014.
4. Томас Х. Кормен, Чарльз И. Лейзерсон, Рональд Л. Ривест, Клиффорд Штайн «Алгоритмы. Построение и анализ». 2013.
5. Дж. Прескилл «Квантовая информация и квантовые вычисления. Том 1». 2008.

6. С. Панасенко «Алгоритмы шифрования», 2008.

СПИСОК ЛИТЕРАТУРЫ

7. Под ред. В.В.Ященко «Ведение в криптографию», 2000.

8. Н.С.Бахвалов, Н.П.Жидков, Г.М.Кобельков «Численные методы». 1987.

9. Ю.В.Нестеренко «Теория чисел», 2008.

10. О.Н.Василенко «Теоретико-числовые алгоритмы в криптографии», 2006.

11. М.П.Минеев, В.Н.Чубариков, «Лекции по арифметическим вопросам криптографии», 2014.

12. В.И.Крупский, В.Е.Плиско «Математическая логика и теория алгоритмов». 2013.

13. Н.П.Редькин «Дискретная математика», 2009.

СПИСОК ЛИТЕРАТУРЫ

14. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, “Handbook of Applied Cryptography”, 2014.

15. Myasnikov A., Shpilrain V., Ushakov A., “Group-based Cryptography”, 2008.

ИНФОРМАЦИЯ О КОМПАНИИ

География «Лаборатории Касперского»

«Лаборатория Касперского» работает почти в **200 странах мира и территориях. Офисы компании расположены в 29 странах.**

KASPERSKY lab

История «Лаборатории Касперского»

1989
Евгений Касперский обнаруживает вирус на своём компьютере. Он пишет программу для его удаления – и это становится его хобби, которое впоследствии вырастет в международный бизнес

1994
Первое международное признание: Университет Гамбурга называет решение Евгения Касперского AntiViral Toolkit Pro лучшим в мире

1997
Основание компании «Лаборатория Касперского» в Москве

1999
Первый зарубежный офис открывается в Великобритании. Впоследствии начнётся масштабная международная экспансия

2000
Начало формирования бренда. Имя основателя компании становится известно во всём мире

2004
«Лаборатория Касперского» становится первой в мире компанией, которая обновляет антивирусные базы каждый час

2010
«Лаборатория Касперского» детектирует первую вредоносную программу для Android и занимает первое место по продажам в розничных сетях в США и третье место в мире

2011
«Лаборатория Касперского» выпускает революционное решение для корпоративных пользователей – Kaspersky Endpoint Security 8

2012
«Лаборатория Касперского» обнаруживает сложнейшие шпионские программы, получившие названия Flame и Gauss

2013
Раскрытие сложных кибершпионских кампаний – «Красный октябрь», NetTraveler и кратковременной таргетированной операции Icefog

KASPERSKY lab

Сотрудники «Лаборатории Касперского»

Мы инвестируем в разработку решений для защиты наших клиентов

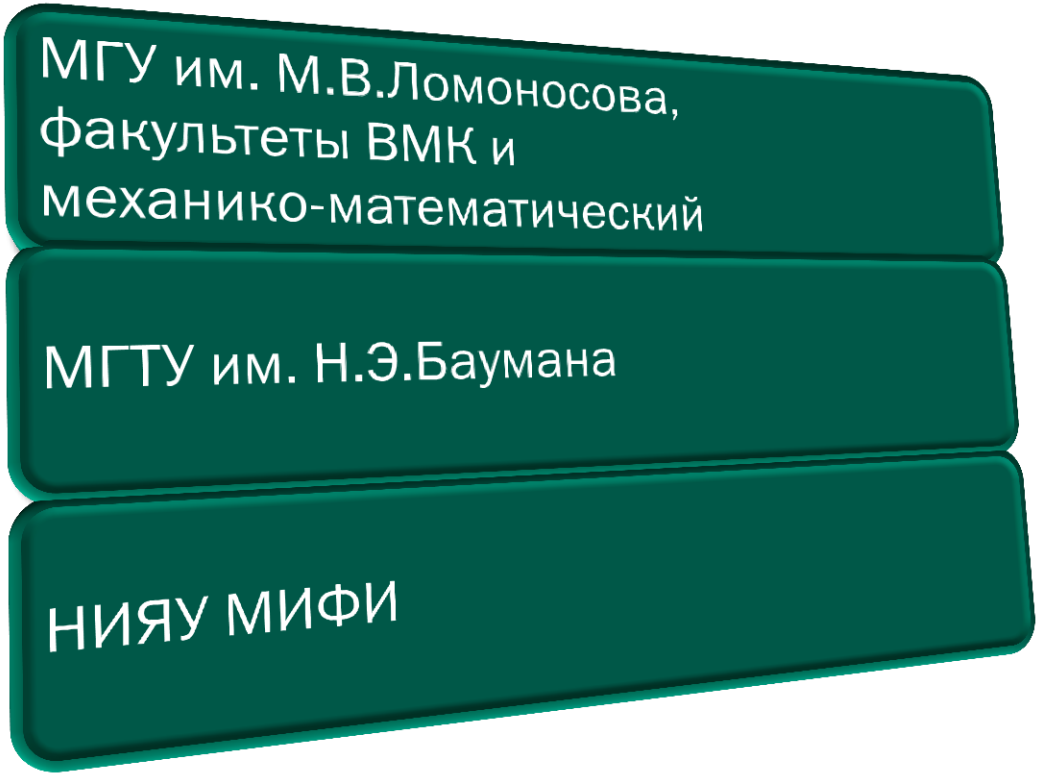
Поэтому треть всех сотрудников компании
– это специалисты в области исследований и разработки

*Данные по состоянию на август 2013 года

KASPERSKY lab

ОБРАЗОВАТЕЛЬНЫЕ ПРОГРАММЫ «ЛАБОРАТОРИИ КАСПЕРСКОГО» (KASPERSKY ACADEMY)

ГДЕ ПРЕПОДАЕМ



ОСЕННИЙ СЕМЕСТР 2015/2016 УЧЕБНОГО ГОДА

- Дистанционные курсы
- Городские олимпиады по информационной безопасности
- ШРД
- Электронные учебники по информационной безопасности
- Международные проекты

ОБЗОР ИНФОРМАЦИОННЫХ УГРОЗ

ДИНАМИКА ПОЯВЛЕНИЯ НОВОГО ВРЕДОНОСНОГО ПО

1995 год: 1 вредоносная программа в час.

2005 год: 1 вредоносная программа в минуту.

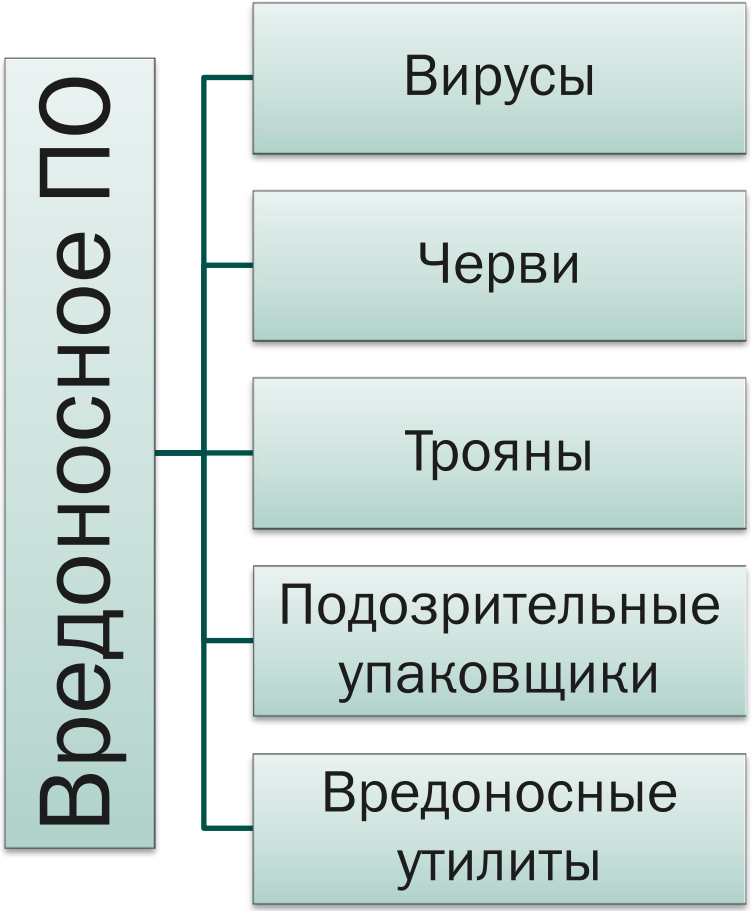
Н. вр.: 2 вредоносные программы в секунду.

ИСТОРИЯ ВРЕДОНОСНОГО ПО

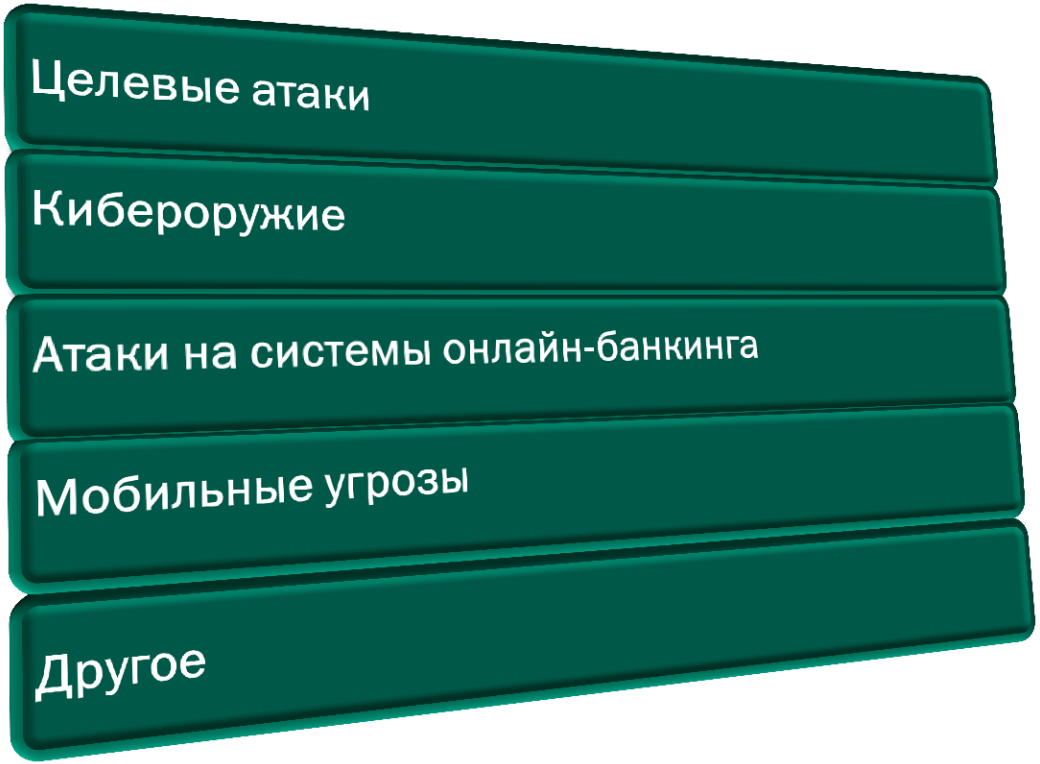
Первые вирусные эпидемии (1981 - 1989): Brain (1986), червь Морриса (1988).

До-интернетовский период и интернет-этап (1990 - 2004): Chameleon (1990), Consept (1995), BackOrifice, Backdoor.BO (1998), Chernobyl (1998), LoveLetter (2000), Slammer (2003).

Современный криминальный этап (2005 – н.вр.)


Вредоносное ПО
Вирусы
Черви
Трояны
Подозрительные упаковщики
Вредоносные утилиты

ГЛОБАЛЬНЫЕ КИБЕРУГРОЗЫ



Целевые атаки	Классические атаки
Цель выбрана специально	Все является целью
Тихие и мгновенные атаки	Массивные и длительные вспышки заражений
Вредоносное ПО более совершенно	Вредоносное ПО менее совершенно и легче детектируется
Атаки остаются незамеченными длительное время	Атаки быстро обнаруживаются

HBGary

DETECT. DIAGNOSE. RESPOND.

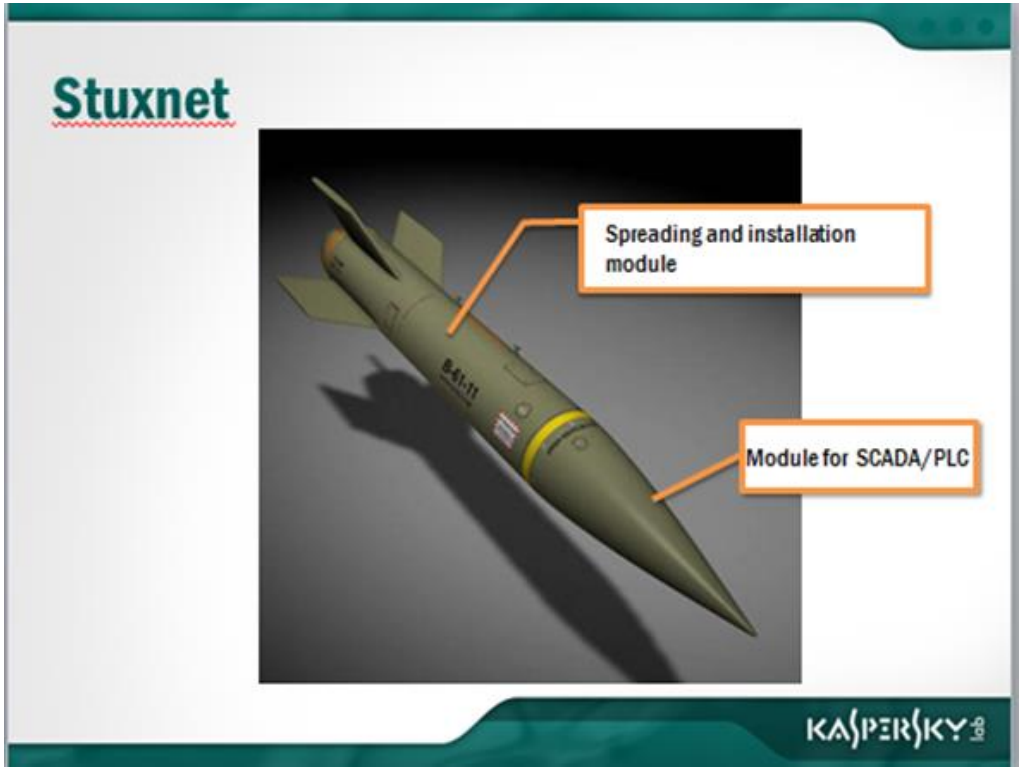
ANONYMOUS

RSA

SECURITY™

KASPERSKY lab

СЕТЕВОЙ ЧЕРВЬ STUXNET (2010)



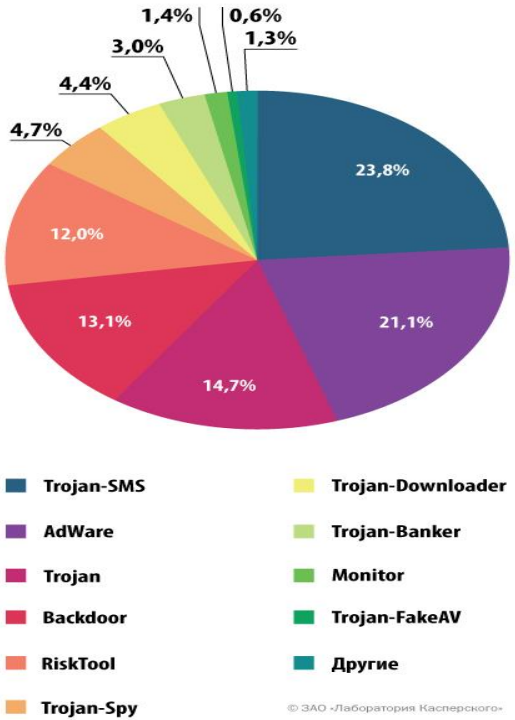
KASPERSKY lab

CARBANAK

KASPERSKY lab

АТАКИ НА БАНКОМАТЫ

СТАТИСТИКА ЗА 2014 ГОД



Распределение мобильных угроз по типам

4, 6 млн вредоносных установочных пакета;

300000 новых мобильных вредоносных программ;

12 000 мобильных банковских троянцев.

KASPERSKY lab

СОВРЕМЕННЫЕ ФИНАНСОВЫЕ ПОТЕРИ МИРОВОЙ ЭКОНОМИКИ ОТ КИБЕРУГРОЗ

Свыше 100 $млрд. в год

- Чистая прибыль Apple: 39,5 $млрд.
- Microsoft: 22 $млрд.
- IBM: 16,9 $млрд.
- Google: 14,4 $млрд.
- BMW: 2,7 млрд. евро
- Toshiba: 0,5 $млрд.
- Сбербанк: 392 млрд. руб.

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab