КИБЕРВОЙНЫ XXI ВЕКА

САМЫЕ ГРОМКИЕ СЛУЧАИ ПРИМЕНЕНИЯ КИБЕРОРУЖИЯ

УТЕЧКА ДАННЫХ ИЗ JPMORGAN CHASE 2014
Крупнейший американский банк, один из старейших финансовых институтов на планете подвергся серьезной хакерской атаке, в результате чего более 83 млн счетов были скомпрометированы. По одной из версий, за нападением стояли русские хакеры, также атаковавшие другие банки США

ТИТАНОВЫЙ ДОЖДЬ 2003–2006
В эту группу специалисты записывают серию атак на американские и британские компании, тесно сотрудничающие с правительством: NASA, Lockheed Martin и другие. Точные масштабы нападения неизвестны, однако в нем подозревают китайских хакеров либо кого-то, кто использовал для этого расположенные на территории Китая компьютеры

НАПАДЕНИЕ НА ЭСТОНИЮ 2007
Серия массированных DDoS-атак на эстонские государственные порталы началась 27 августа, сразу после решения правительства перенести статую бронзового солдата в Таллине. В организации нападения некоторые специалисты обвиняют структуры, близкие к движению «Наши»

СУХУМИ 2009
Прогрузинский блогер Сухуми, принимавший активное участие в информационной войне между Россией и Грузией в 2008 году, был выбран главной целью хакеров, сумевших «положить» 7 августа на пару часов платформы Facebook, Google Blogger, LiveJournal и Twitter

НАПАДЕНИЕ НА КОРЕЮ 2009
Более 166 тыс. компьютеров были инфицированы вирусом, сделавшим их частью огромного ботнета, чей атакующий потенциал был направлен против правительственных, финансовых и медийных сайтов Южной Кореи

ОПЕРАЦИЯ ABABIL 2012
Общее название для серии кибератак на американские финансовые институты, инициированной группировкой Cyber fighters of Izz Ad-Din Al Qassam, названной в честь мусульманского проповедника

АЭС В БУШЕРЕ, ИРАН 2010
По версии New York Times, компьютерный червь Stuxnet был разработан спецслужбами США и Израиля специально для саботажа иранской ядерной программы. По данным Symantec, вирусом оказалось заражено 58,85% компьютеров Ирана, 18,22% компьютеров Индонезии и 8,31% машин в Индии

АТАКА НА БИРМУ 2010
Мощнейшая DDoS-атака на крупнейшего интернет-провайдера Бирмы началась незадолго до первых за 20 лет всеобщих выборов, впоследствии признанных фиктивными

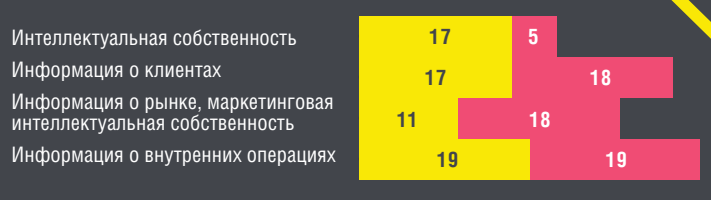
ОПЕРАЦИЯ «АВРОРА» 2009
Серия кибератак, инициированных в 2009 году структурами, близкими к Китайской народной освободительной армии, против американских интернет-гигантов, по большей части Google

АТАКА «МЕССИИ» 2013
1 июня государственными регуляторными органами Сингапура были приняты новые правила: в течение 24 часов все местные сайты с посещаемостью от 50 тыс. посетителей должны были удалить с серверов любые статьи, призывающие к «нарушению расовой либо религиозной гармонии» в стране. В ответ на это хакерская группировка «Анонимусы» инициировала атаку на государственные сайты Сингапура, в том числе сайт премьер-министра.

ОПЕРАЦИЯ CLEAVER 2014
Согласно отчету компании Cylance, к массовой атаке на 50 объектов из 16 стран (в том числе Korean Air, Qatar Airlines, Pemex) оказались причастны иранские хакеры, тесно связанные с Корпусом стражей исламской революции

АТАКИ НА КРИТИЧЕСКУЮ ИНФРАСТРУКТУРУ

ОСНОВНЫЕ ПРИЧИНЫ ИНЦИДЕНТОВ В ИНДУСТРИАЛЬНЫХ СЕТЯХ (%)



КАКИЕ ДАННЫЕ У ВАС БЫЛИ УКРАДЕНЫ?

ГИБРИДНАЯ ВОЙНА

КОНВЕНЦИОНАЛЬНЫЕ ВОЕННЫЕ ДЕЙСТВИЯ

Обычная война

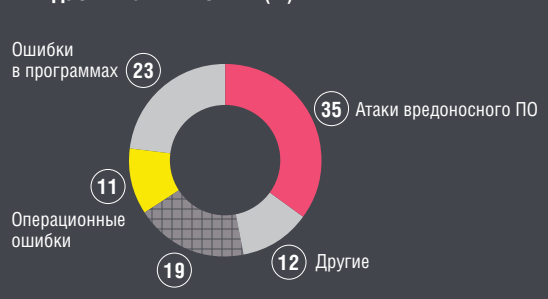
Малая война
(разведывательные, диверсионные, террористические действия малых подразделений; уязвимые цели: мобильные устройства госслужащих; АСУ иностранного производства)

КИБЕРВОЙНА

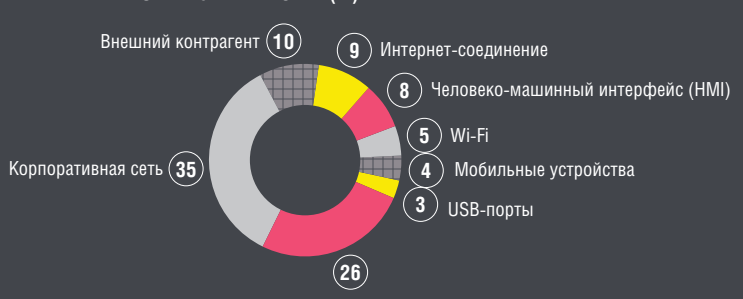
Применение кибероружия

Новые методы пропаганды и дезинформации
(крайне эффективны через социальные медиа)

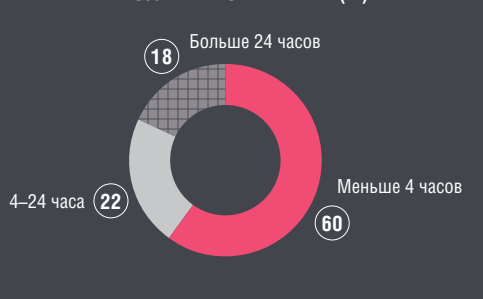
ОСНОВНЫЕ ПРИЧИНЫ ИНЦИДЕНТОВ В ИНДУСТРИАЛЬНЫХ СЕТЯХ (%)



ТОЧКИ ПОПАДАНИЯ ВРЕДОНОСНОГО ПО В ПРОМЫШЛЕННЫЕ СЕТИ (%)



ВРЕМЯ БЕЗДЕЙСТВИЯ СИСТЕМЫ В РЕЗУЛЬТАТЕ ЗАРАЖЕНИЯ (%)



ИСТОЧНИКИ: SECURITYINCIDENTS.NET, KASPERSKY LAB, 2014.