

Информационная безопасность в финансовом секторе

Тренды 2015

Михаил Козлов

CNews: «Информационная
безопасность в финансовом секторе:
угрозы и противодействие»

09 апреля 2015

Тренды 2015

РЫНОК
Новое регулирование
Импортозамещение

- У нас дыра в безопасности.
- Слава богу, хоть что-то у нас в безопасности...

Atkritka.com

Ущерб?

// **СМИ: хакеры похитили \$300 млн со счетов более ста банков, в том числе российских**



Международная группировка хакеров похитила со счетов более ста банков, большинство из которых находится в России, сотни миллионов долларов. Об этом сообщила газета [The New York Times](#), в распоряжение которой попал доклад российской компании «Лаборатория Касперского». Преступной группировке, в которую входили хакеры из РФ, Китая и европейских стран, удалось внедрить в компьютерные системы банков в 30 странах вредоносное программное обеспечение. С его помощью злоумышленники получили закрытую информацию о работе финансовых учреждений и на протяжении почти двух лет переводили миллионы долларов с их счетов на свои подставные счета в США и Китае, сообщает 15 февраля ТАСС.

Ущерб?

// Совет безопасности России решил создать центр реагирования на инциденты информационной безопасности в финансовой сфере, который будет называться FinCERT

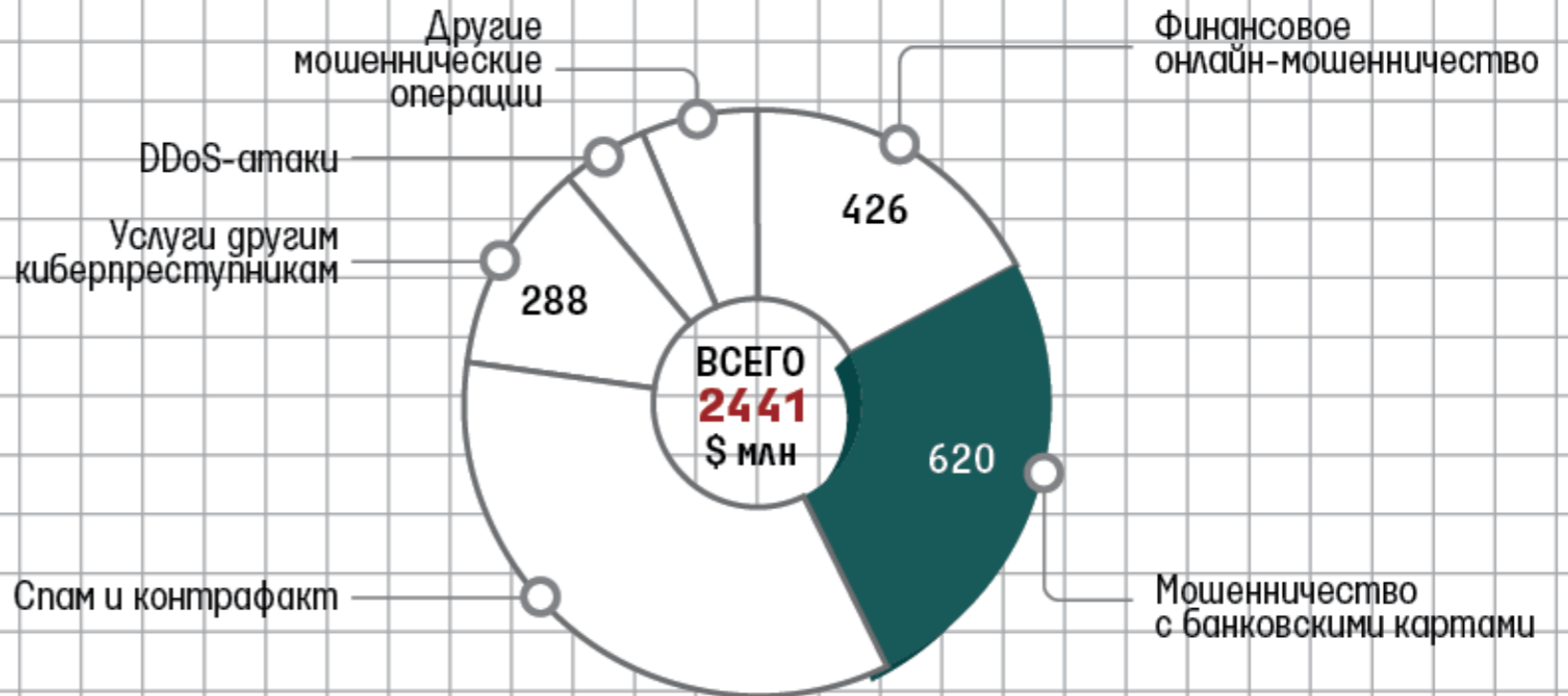
Источник: [Ведомости](#) 30/01/2015

Совет безопасности России поручил Центробанку запустить работу Центра борьбы с киберугрозами (FinCERT) в срок до 1 мая 2015 года

Источник: [Известия](#) 30/03/2015

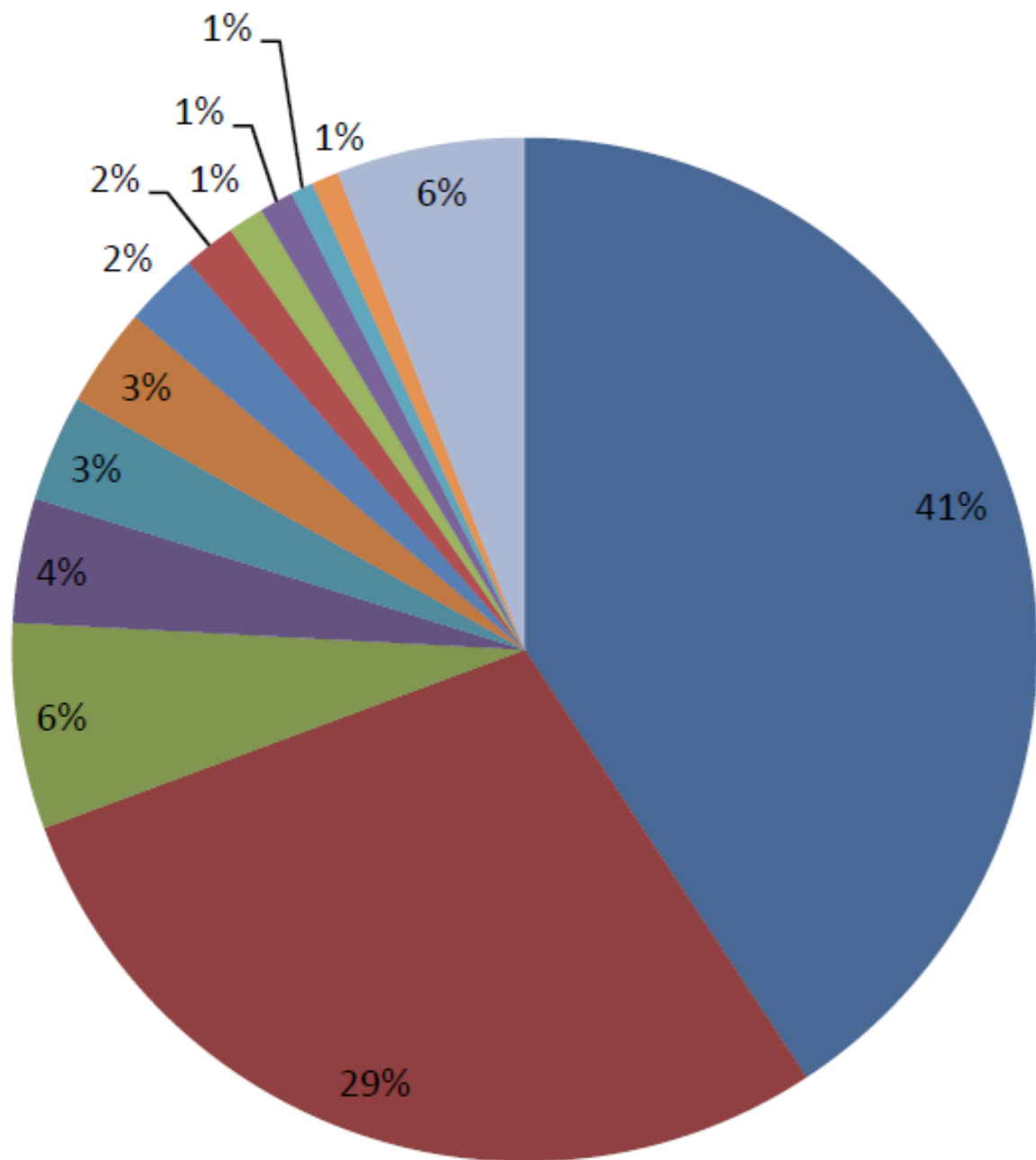
Ущерб от киберпреступности

Структура российского «рынка» киберпреступности в России в 2013 г.



ИСТОЧНИК: GROUP-IB

Рынок ИБ в РФ



- 41% Рынок сетевой безопасности
- 29% Рынок систем антивирусной защиты
- 06% Рынок аппаратных средств двухфакторной аутентификации

\$1,4 млрд.

РЫНОК ИБ В РФ

J'son & Partners (средства и услуги ИБ):

- 51 млрд. руб. в 2014 \$1,32 млрд.
- 7% ИТ-рынка
- 45 млрд. руб. в 2013 (рост 13%) \$1,41 млрд.

Ущерб заметно больше рынка ИБ!

\$2,44 vs. \$1,4 млрд. (2013)

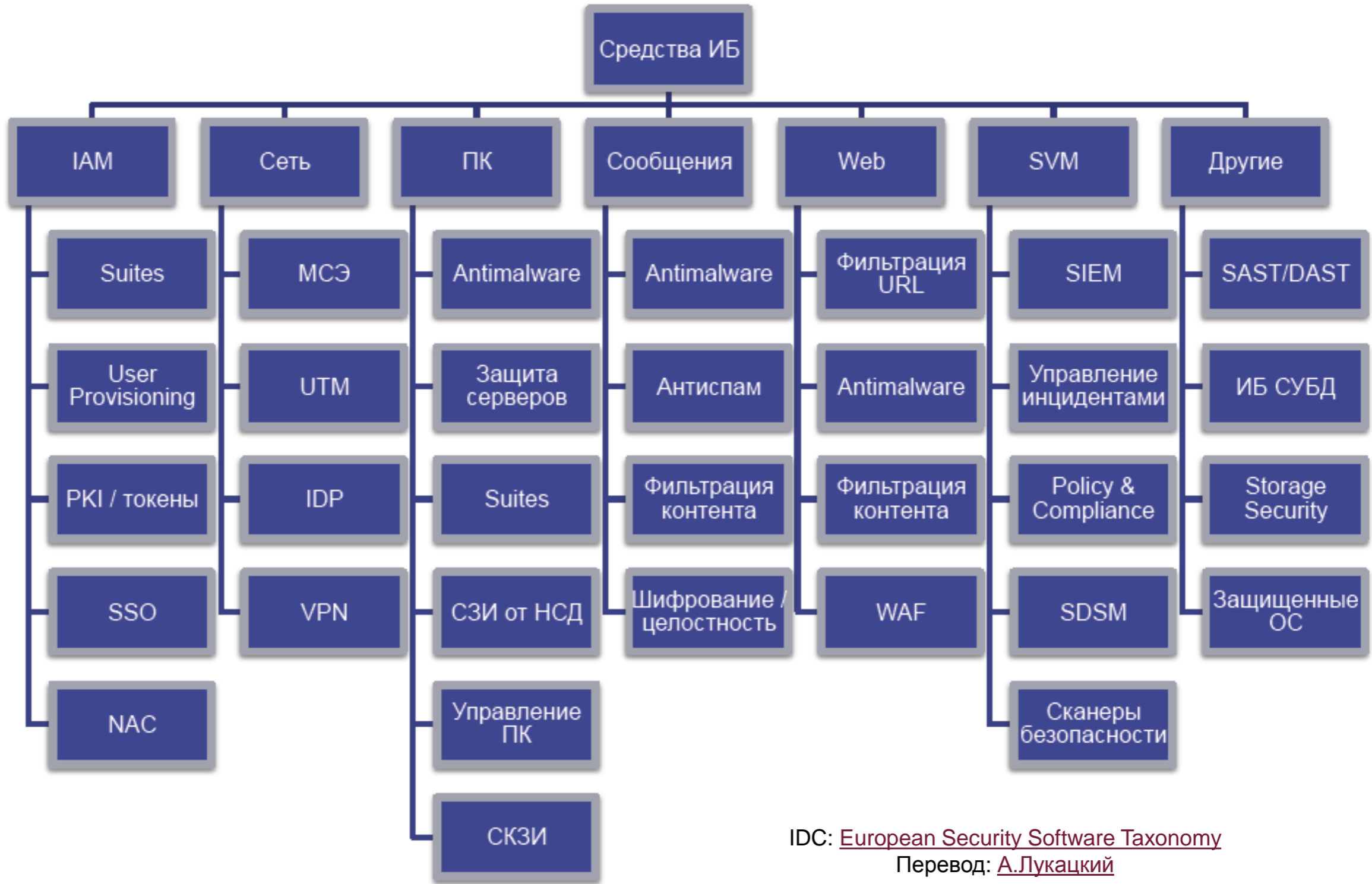
Помогают ли вам регуляторы?

АР, УП, ПП, ГОСТы,
НМД ЦБ (СТО, П, РС, FinCERT,
Basel III...), СОПКА, НМД ФСТЭК,
БД угроз безопасности
информации (ФСТЭК), НМД ФСБ,
НМД РКН, PCI DSS, FATCA...

Безопасность ДБО?

// Разработчики систем ДБО не были готовы к тому, что их продукт будут ломать хакеры. У разработчиков отсутствуют процессы разработки безопасного кода.

Импортозамещение в ИБ



Мнение про отечественное ИБ



Российский рынок средств защиты развит слабо и, преимущественно, «закрывает» регулятивные требования

Наиболее развит рынок antimalware, СКЗИ/VPN, DLP и защищенных ОС

В большинстве ниш рынка ИБ присутствует всего 1-2 игрока, что недостаточно для адекватного выбора и нормальной конкуренции

Функциональность, качество и возможность массового производства средств защиты отечественного производства на данный момент сильно уступают зарубежным аналогам

Спектр игроков ИБ, предлагающих широкий спектр средств защиты, невелик: ЛК, InfoWatch, Positive Technologies, Эшелон

Источник: [А.Лукацкий](#)

Мнение про Открытое ПО

// «Открытое – значит российское»

✘ 85 % изменений в ядре Linux внесены западными вендорами (включая АНБ)

84,6%
Программисты,
получающие
за эту работу
оплату

13,6%
Энтузиасты

0,9%
Образователь-
ные учрежде-
ния

0,9%
The Linux
Foundation



Вопросы для обсуждения

- ✓ Что нужно делать для повышения защищенности финансовых ИТ?
- ✓ Как существующая нормативная база в области ИБ и ПДн помогает вам решать задачи безопасности?
- ✓ Готовы ли заказчики к импортозамещению в ИБ?
- ✓ Волнует ли вас ИБ в облаках, мобильности, Big Data, Интернете Вещей?





Михаил Козлов

www.devbusiness.ru/mkozloff

