

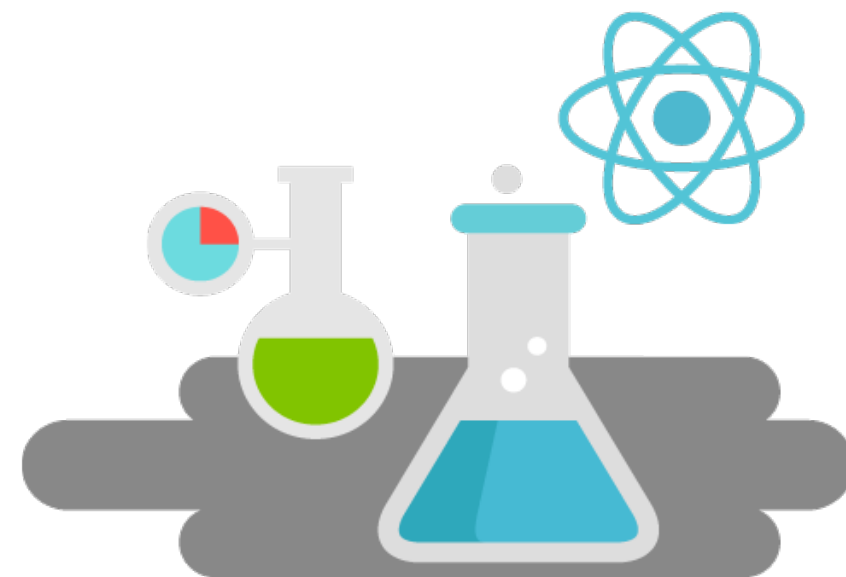
СОВРЕМЕННЫЕ КИБЕРУГРОЗЫ И СПОСОБЫ ЗАЩИТЫ

Жанибек Шутбаев
ESET Kazakhstan



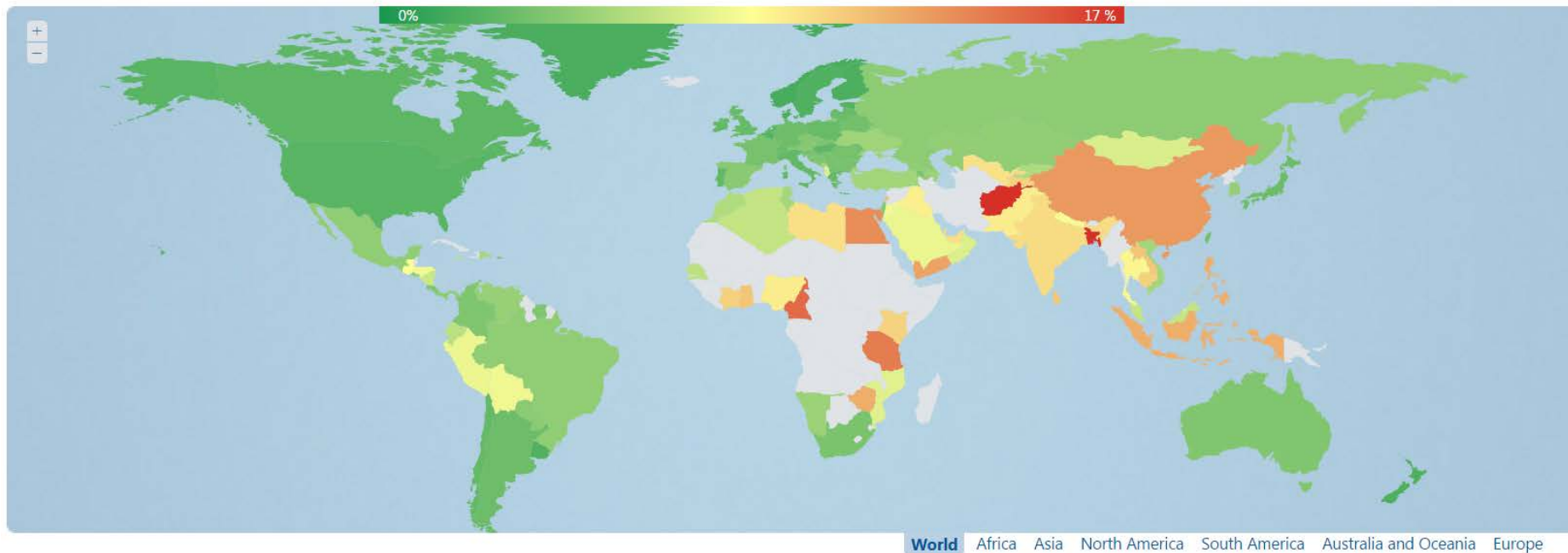
ВИРУСНАЯ ЛАБОРАТОРИЯ ESET

- **500 000** образцов вредоносного ПО каждый день
- **200** образцов мобильных угроз каждый месяц
- В **2014-2015** гг. фиксируется вредоносное ПО для всех устройств: POS-терминалы, банкоматы, роутеры, носимые устройства
- Двухкратный рост числа APT-атак в **2014-2015** гг.
- **ТОП-3** вектора атак: e-mail, 0day, эксплойты



ВИРУСНАЯ ЛАБОРАТОРИЯ ESET

eset VIRUS RADAR BETA



Пример сложного вектора атак

FINDPOS

- Внедряет свой код в процесс, отвечающий за получение информации с магнитной ленты банковской карты
- Отправка скопированных из памяти данных на удаленный сервер (exfiltration) выполняется с использованием POST-запроса HTTP-протокола
- Данные перед отправкой переименовываются

```

push 58h
push offset stru_41AE88
call SER_prolog5_GS
mov ebx, ecx
lea eax, [ebp+SystemInfo]
push eax ; lpSystemInfo
call ds:GetSystemInfo
push ebx ; dwProcessId
push 0 ; bInheritHandle
push 410h ; dwDesiredAccess
call ds:OpenProcess
mov edi, eax
mov [ebp+hProcess], edi
test edi, edi
js short loc_401C4E

and [ebp+ms_exc.registration.TryLevel], 0
mov esi, [ebp+SystemInfo.lpMinimumApplicationAddress]
mov [ebp+var_64], esi

loc_401BF6:
push 1Ch ; dwLength
lea eax, [ebp+Buffer]
push eax ; lpBuffer
push esi ; lpAddress
mov edi, [ebp+hProcess]
push edi ; hProcess
call ds:VirtualQueryEx
cmp eax, 1Ch
jnz short loc_401C3E

cmp [ebp+Buffer.State], 1000h
jnz short loc_401C2A

test byte ptr [ebp+Buffer.Protect], 4
jz short loc_401C2A

push [ebp+Buffer.RegionSize] ; nSize
push esi ; lpBaseAddress
mov ecx, ebx
mov ecx, edi
call read_memory
pop ecx
pop ecx

loc_401C2A:
add esi, [ebp+Buffer.RegionSize]
mov [ebp+var_64], esi
cmp esi, [ebp+SystemInfo.lpMaximumApplicationAddress]
jb short loc_401BF6

jmp short loc_401C3E

loc_401C3B:
; Exception handler 0 for function 401BDD
mov esp, [ebp+ms_exc.old_esp]

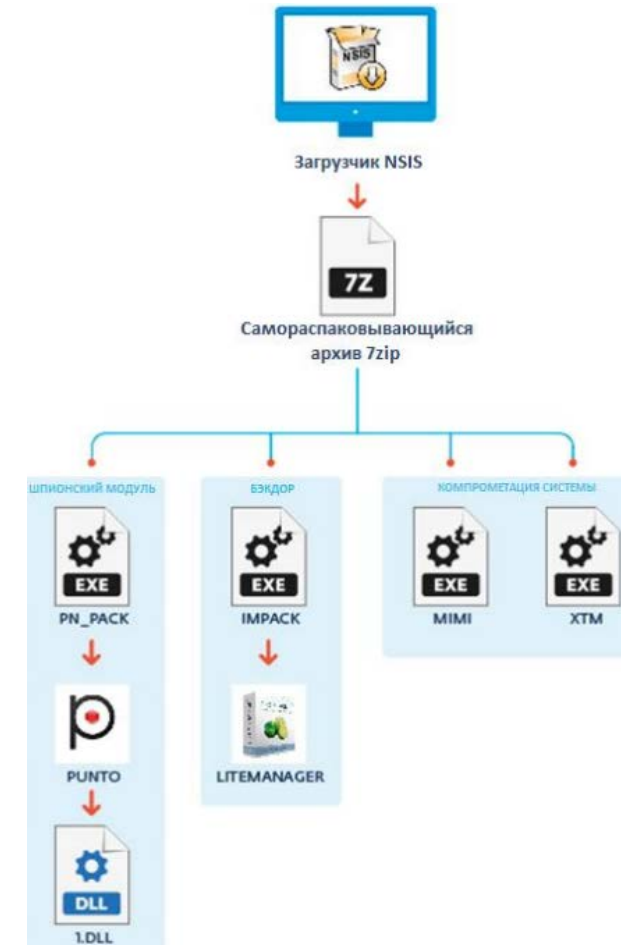
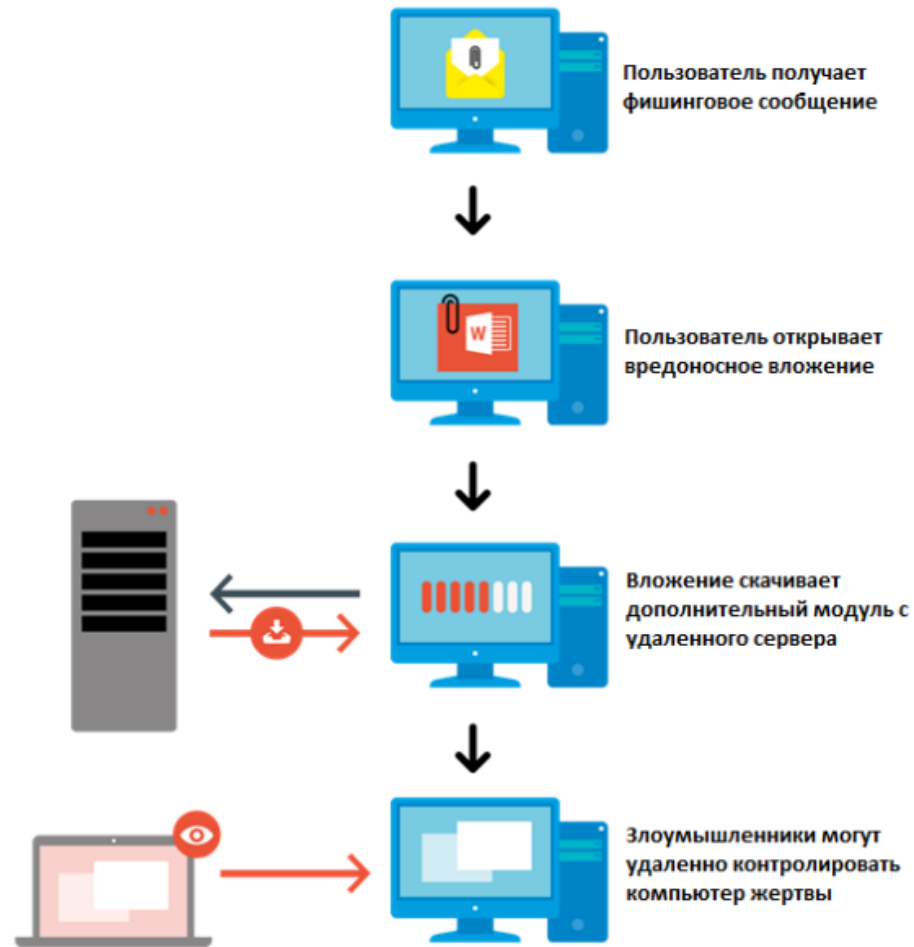
loc_401C3E:
mov [ebp+ms_exc.registration.TryLevel], 0FFFFFFFh
push [ebp+hProcess] ; hObject
call ds:CloseHandle

```

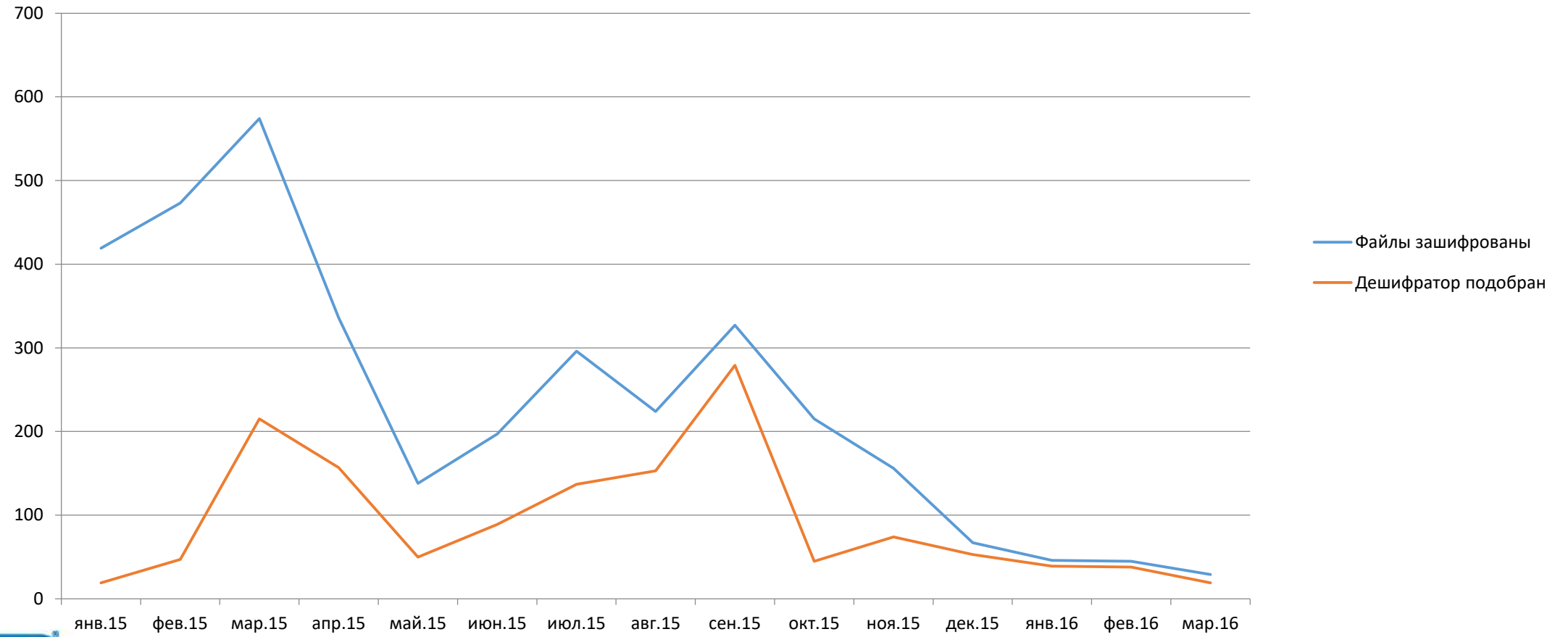
ШИФРАТОРЫ



СЦЕНАРИЙ ЗАРАЖЕНИЯ



ШИФРАТОРЫ



КИБЕРАТАКИ



ВОСТОЧНАЯ ЕВРОПА – В ЦЕНТРЕ КИБЕРАТАК

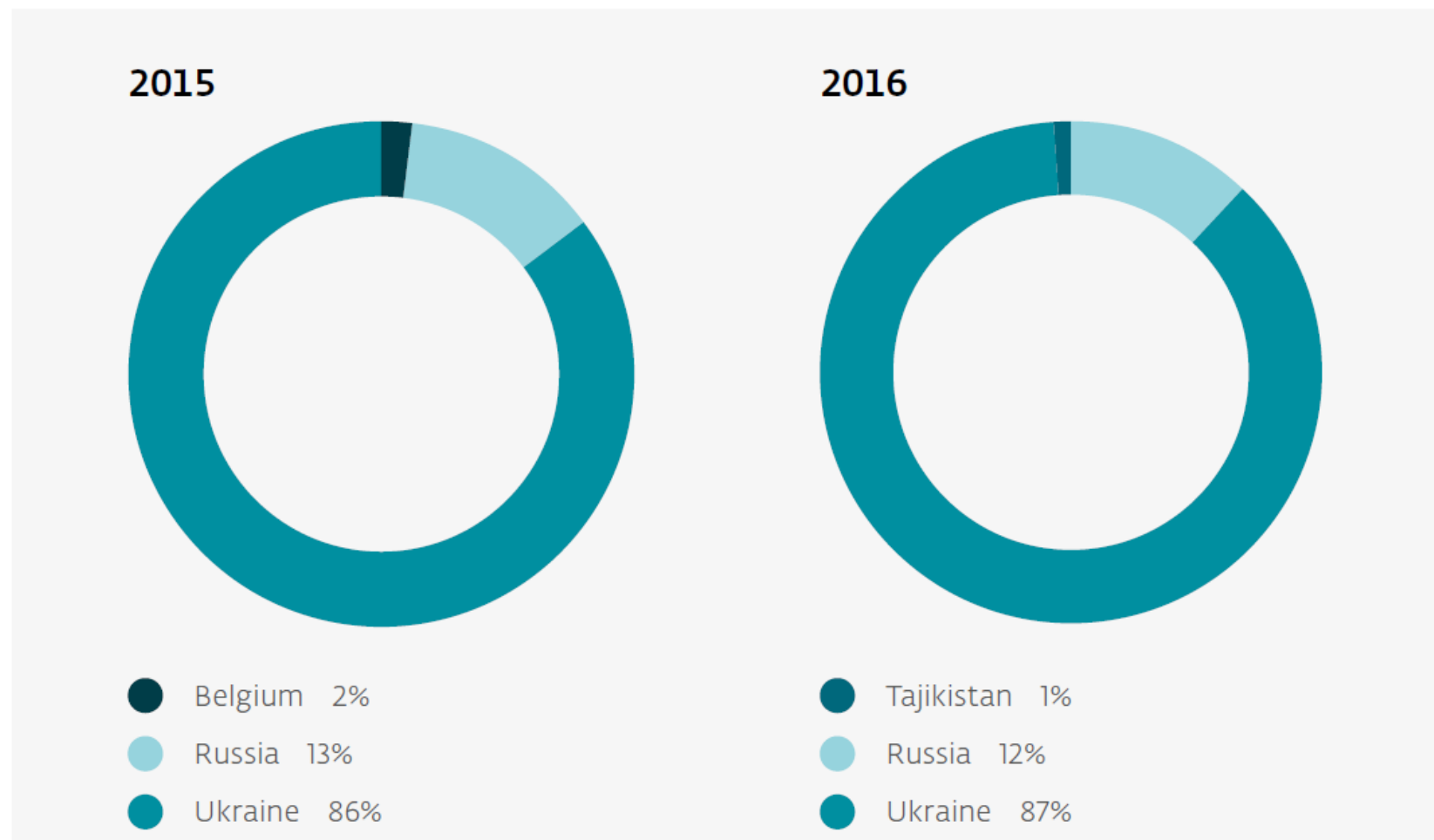


Operation Buthrap you say?



АТАКИ НА ГОССЕКТОР И КИБЕРШПИОНАЖ

*Операция
«Прикормка»*



АТАКИ НА БАНКИ

«Ловушка для бухгалтера»



Пользователь
получил спам



Открывает
зараженный
word-файл



Файл
скачивает
допмодуль



За жертвой
можно
следить

АТАКИ НА ЭНЕРГЕТИКУ

- Более **60%** сотрудников открыли зараженные файлы.
- **38%** выслали личную и конфиденциальную информацию.
- Сотрудники ИТ и ИБ также попали в первые два пункта.



ПРОДУКТЫ ESET



РАБОЧИЕ
СТАНЦИИМОБИЛЬНЫЕ
УСТРОЙСТВАФАЙЛОВЫЕ
СЕРВЕРЫПОЧТОВЫЕ
СЕРВЕРЫ

ШЛЮЗЫ

ЦЕНТРАЛИЗОВАННОЕ
УПРАВЛЕНИЕ

ESET NOD32 SECURE ENTERPRISE

ESET NOD32 SMART SECURITY BUSINESS EDITION

ESET NOD32 BUSINESS EDITION

ESET NOD32 MAIL SECURITY FOR MICROSOFT EXCHANGE

ESET NOD32 MAIL SECURITY FOR LINUX/BSD/SOLARIS

ESET NOD32 ANTIVIRUS FOR LOTUS DOMINO

ESET NOD32 FOR KERIO CONNECT

ESET NOD32 GATEWAY SECURITY FOR LINUX/BSD/ SOLARIS

ESET NOD32 FOR KERIO CONTROL



**MITSUBISHI
MOTORS**

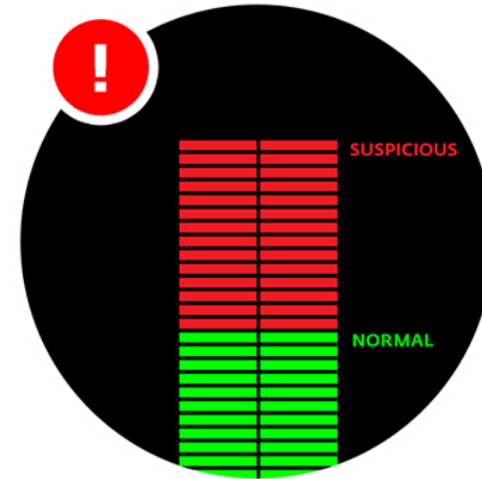
Антифишинг



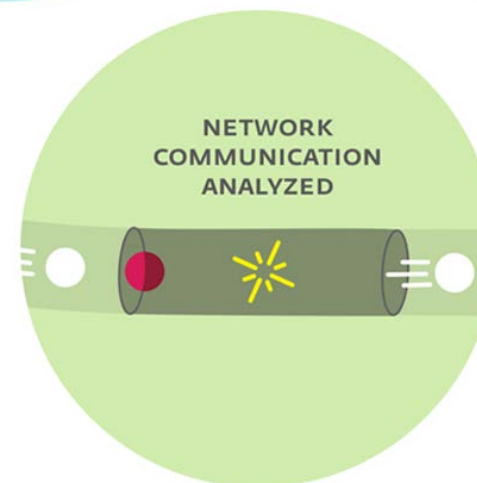
*Защита от
эксплойтов*



*Расширенное
сканирование памяти*



*Защита от
ботнетов*



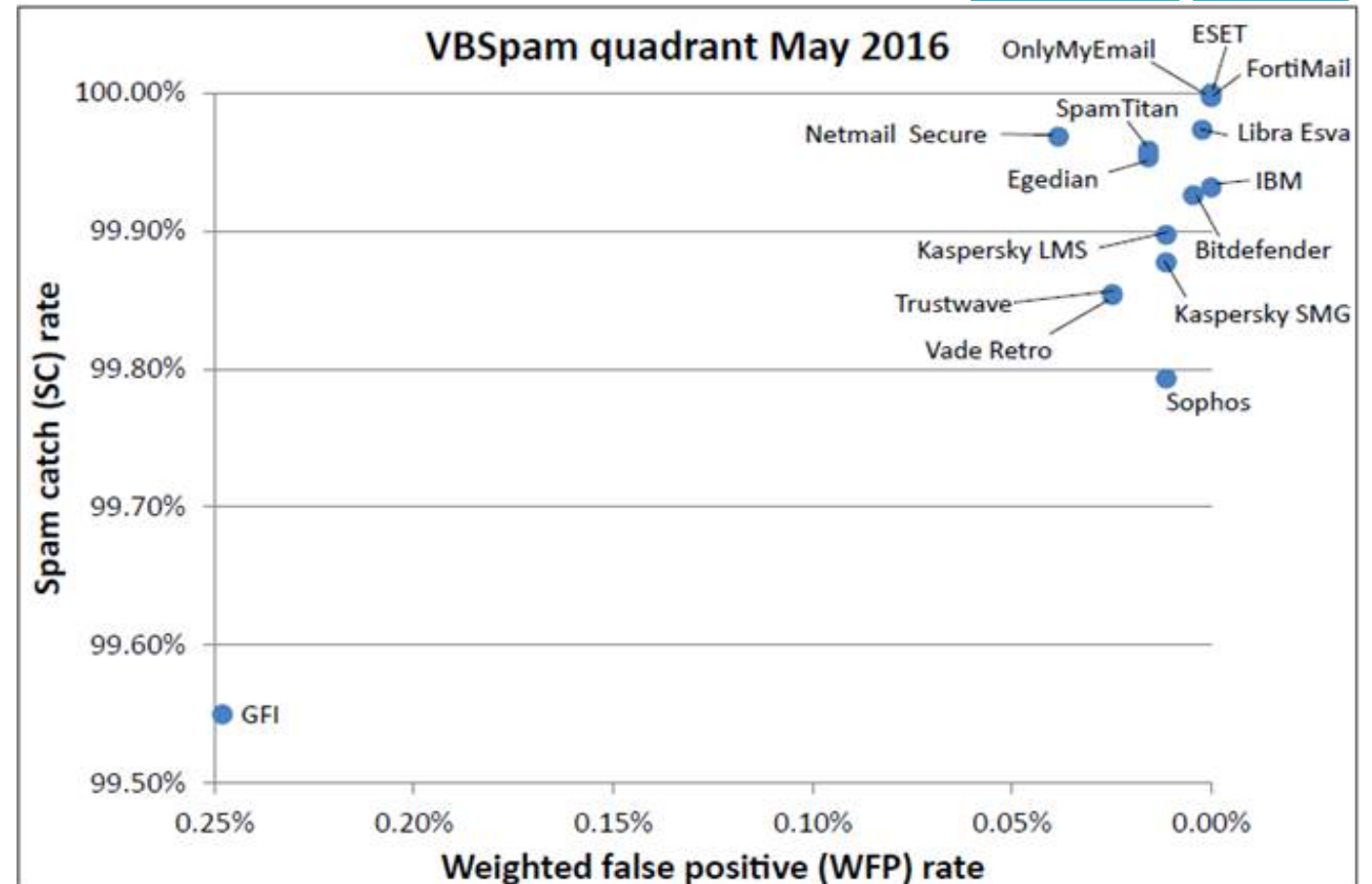
*Щит
уязвимости*



ЗАЩИТА ПОЧТЫ – отражение 90% атак

ESET Mail Security for Exchange

- Антивирусная защита
- Антиспам
- Централизованное управление



СПАСИБО ЗА ВНИМАНИЕ

