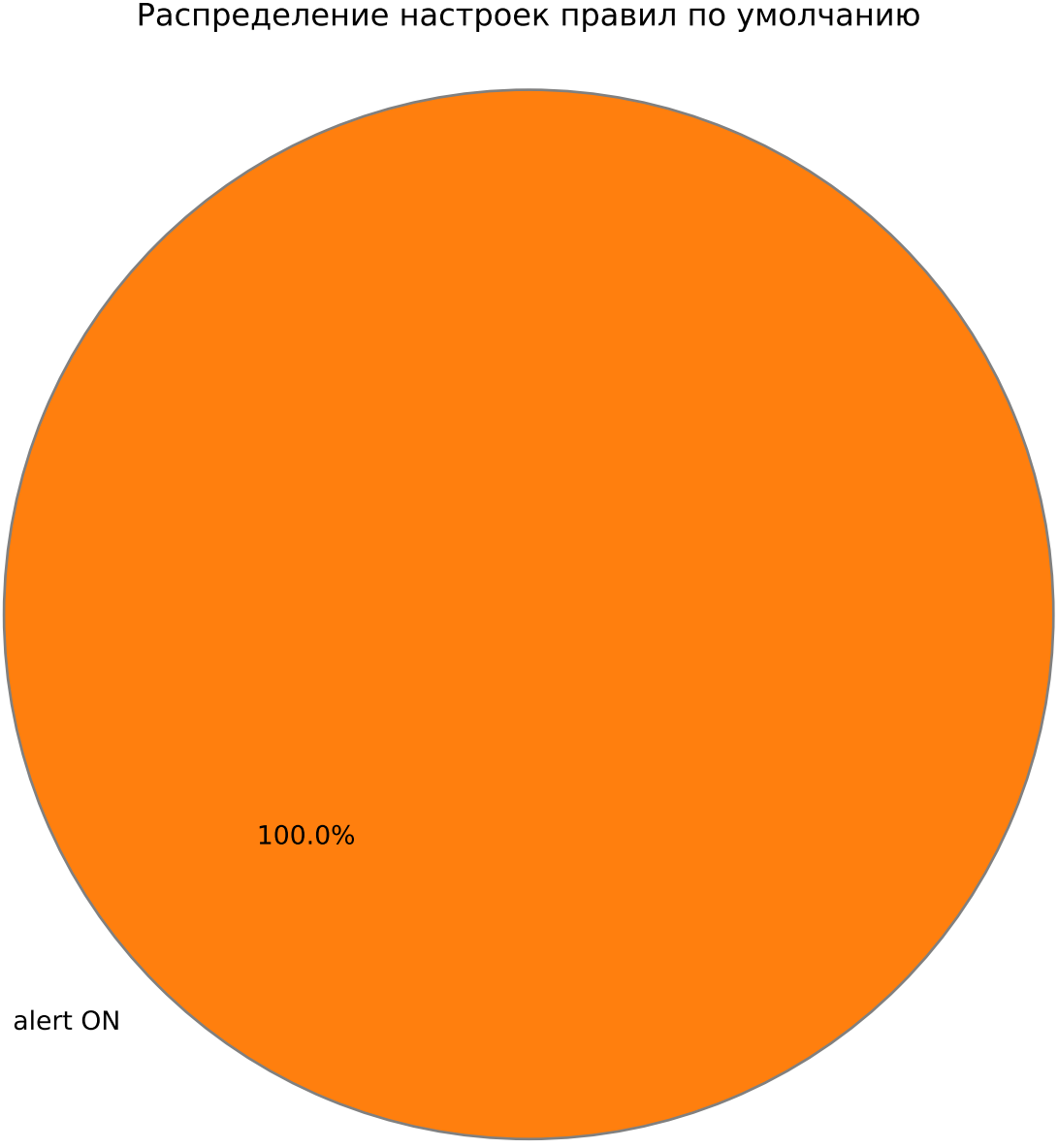
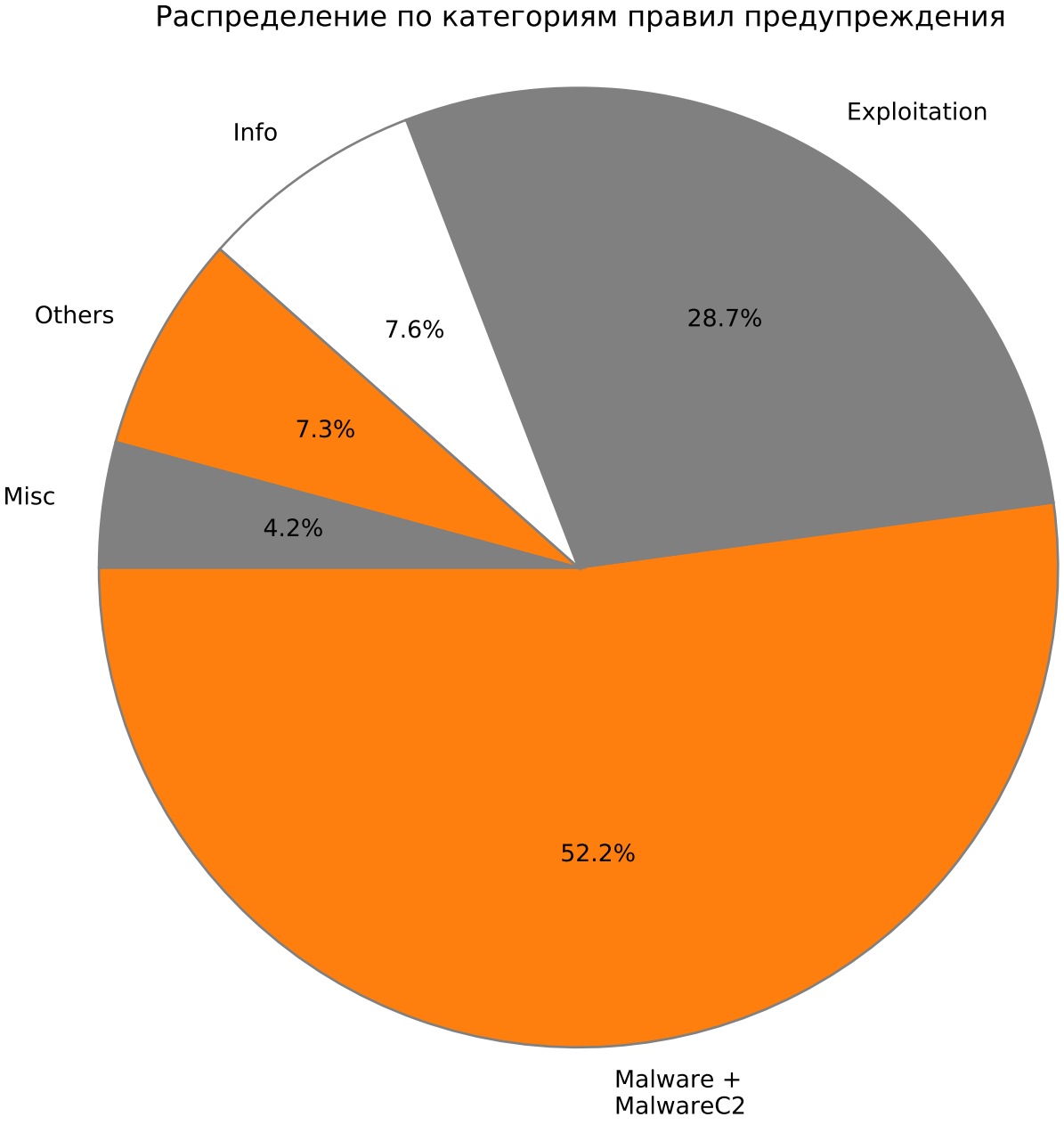
Отчёт о составе БРП AM Rules АО "ПМ" от 2022-07-18


Распределение настроек правил по умолчанию
100.0%
alert ON

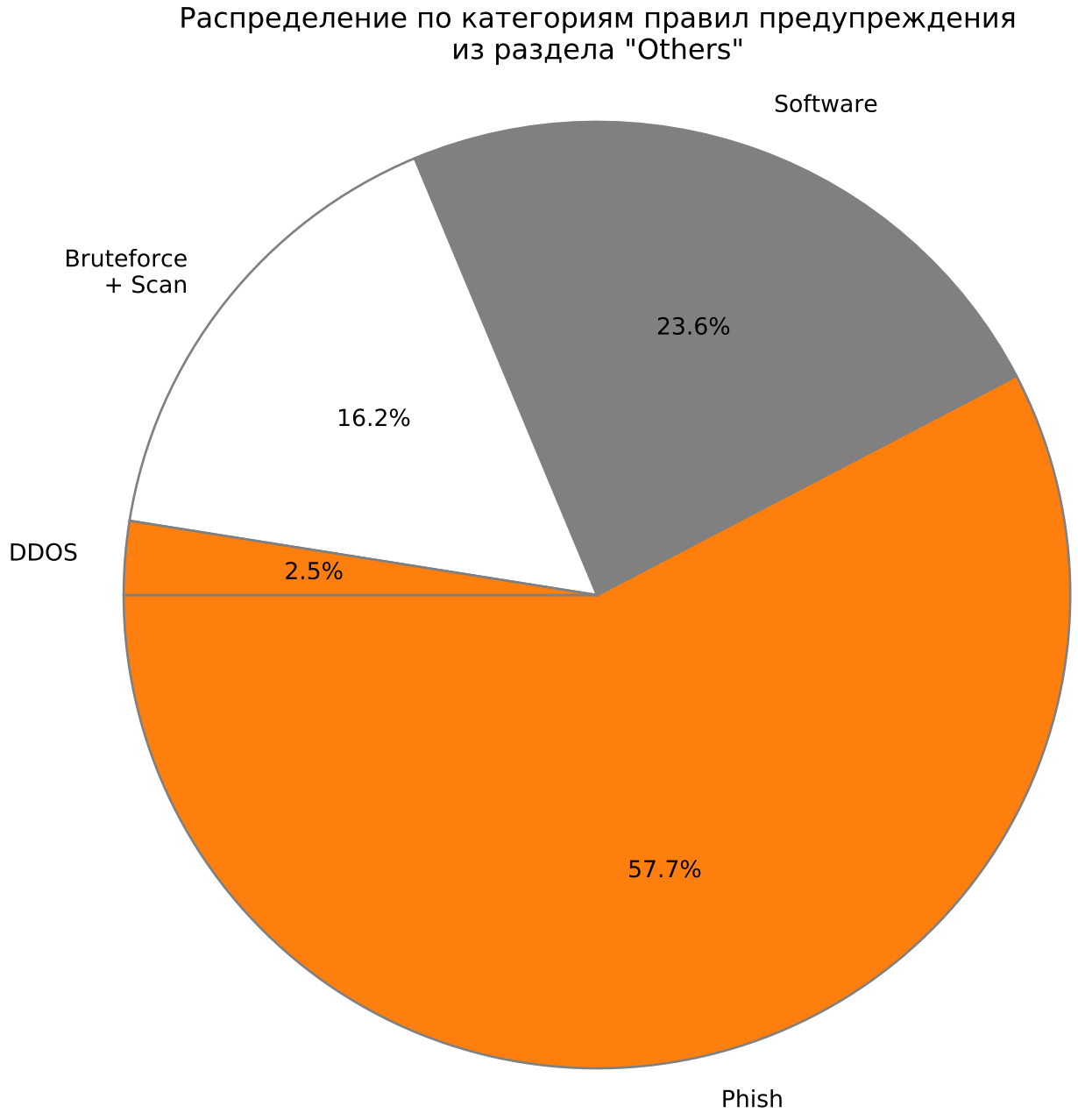
alert ON	29864

alert ON - правило поставляется во включённом состоянии
alert OFF - правило поставляется в выключенном состоянии, клиент может включить его самостоятельно


Распределение по категориям правил предупреждения
Exploitation
28.7%
Info
7.6%
Others
7.3%
Misc
4.2%
52.2%
Malware +
MalwareC2

Malware + MalwareC2	15580
Exploitation	8565
Info	2268
Others	2192
Misc	1259

Malware+MalwareC2 - активность вредоносного ПО
Exploitation - атаки на уязвимости
Info - информационные правила дополнительного контекста
Others - правила, не попадающие в крупные категории.
Их распределение представлено на следующем слайде


Распределение по категориям правил предупреждения
из раздела "Others"
Software
23.6%
Bruteforce
+ Scan
16.2%
DDOS
2.5%
57.7%
Phish

Phish	1264
Software	518
Bruteforce + Scan	355
DDOS	55

Phish - активность, указывающая на фишинг
Software - использование подозрительного или многоцелевого ПО
Bruteforce+Scan - попытки подбора пароля или сканирования сети
DDOS - активность с признаками распределённой атаки
на отказ в обслуживании


Распределение по профилям защиты
Рабочие станции
68.4%
13.1%
Веб-серверы
6.0%
Все профили
3.6%
3.6%
Специализированные профили
3.3%
Клиент-серверное ПО
2.0%
Серверы
Сетевое оборудование

Рабочие станции	20421
Веб-серверы	3912
Все профили	1784
Специализированные профили	1090
Клиент-серверное ПО	1081
Серверы	982
Сетевое оборудование	594