Адаптивная под условия продолжительного мониторинга **система визуализации** событий информационной безопасности

Елизаров А.В.
к.ф.-м.н., с.н.с., заведующий лабораторией Гамаюнов Д.Ю.

МГУ

INFORMATION SYSTEMS SECURITY LAB
SECLAB
лаборатория Безопасности Информационных Систем

ВМиК

ИНТЕРФЕЙСЫ СОИБ НЕЭФФЕКТИВНЫ

А НУЖНО ПРИНИМАТЬ ПРАВИЛЬНЫЕ РЕШЕНИЯ БЫСТРО

ОПЕРАТОР — «БУТЫЛОЧНОЕ ГОРЛЫШКО» СОИБ

ОН НЕ ВОСПРИНИМАЕТ ТОТ ОБЪЕМ ИНФОРМАЦИИ, КОТОРЫМ МАНИПУЛИРУЕТ СОИБ

ОПЕРАТОР УСТАЕТ В ТЕЧЕНИЕ ДНЯ

И ЕГО ПРОИЗВОДИТЕЛЬНОСТЬ СНИЖАЕТСЯ

МОЖНО УПРАВЛЯТЬ НАГРУЗКОЙ НА ОПЕРАТОРА

АДАПТАЦИЯ КОГНИТИВНОЙ НАГРУЗКИ ПОВЫШАЕТ ЭФФЕКТИВНОСТЬ ОПЕРАТОРА

МОЖНО ОПРЕДЕЛЯТЬ УРОВЕНЬ ЗАГРУЖЕННОСТИ ОПЕРАТОРА

ПО ХАРАКТЕРИСТИКАМ ЕГО ВЗАИМОДЕЙСТВИЯ С ИНТЕРФЕЙСОМ

СОИБ (анг. SIEM) — Система Обеспечения Информационной Безопасности


ЖУРНАЛЫ СОБЫТИЙ
АНТИВИРУСЫ
СКАНЕРЫ УЯЗВИМОСТЕЙ
IDS и IPS
СОИБ
DLP
СЕТЕВОЕ ОБОРУДОВАНИЕ
СИСТЕМЫ КОНТРОЛЯ И
УПРАВЛЕНИЯ ДОСТУПОМ

ЖУРНАЛЫ СОБЫТИЙ

АНТИВИРУСЫ

IDS

DLP

СЕТЕВОЕ ОБОРУДОВАНИЕ

С

УПРАВЛЕНИЯ ДОСТУПОМ

СКАНЕРЫ УЯЗВИМОСТЕЙ

НАБЛЮДЕНИЕ

СОИБ ⇄ ОПЕРАТОР

РЕАГИРОВАНИЕ

СОИБ

ALIEN VAULT — **5,000** СОБЫТИЙ/СЕКУНДУ

ArcSight An HP Company — **12,500** СОБЫТИЙ/СЕКУНДУ

Radar — от **5,000** СОБЫТИЙ/СЕКУНДУ

McAfee — до **300,000** СОБЫТИЙ/СЕКУНДУ

ЖУРНАЛЫ СОБЫТИЙ

АНТИВИРУСЫ

IDS

СОИБ ОПЕРАТОР

DLP

СЕТЕВОЕ ОБОРУДОВАНИЕ

С

УПРАВЛЕНИЯ ДОСТУПОМ

СКАНЕРЫ УЯЗВИМОСТЕЙ

ИНТЕРФЕЙС

СОИБ

ОПЕРАТОР

ИНТЕРФЕЙС

ЦЕЛЬ

ВЕРНЫЕ РЕШЕНИЯ БЫСТРЕЕ

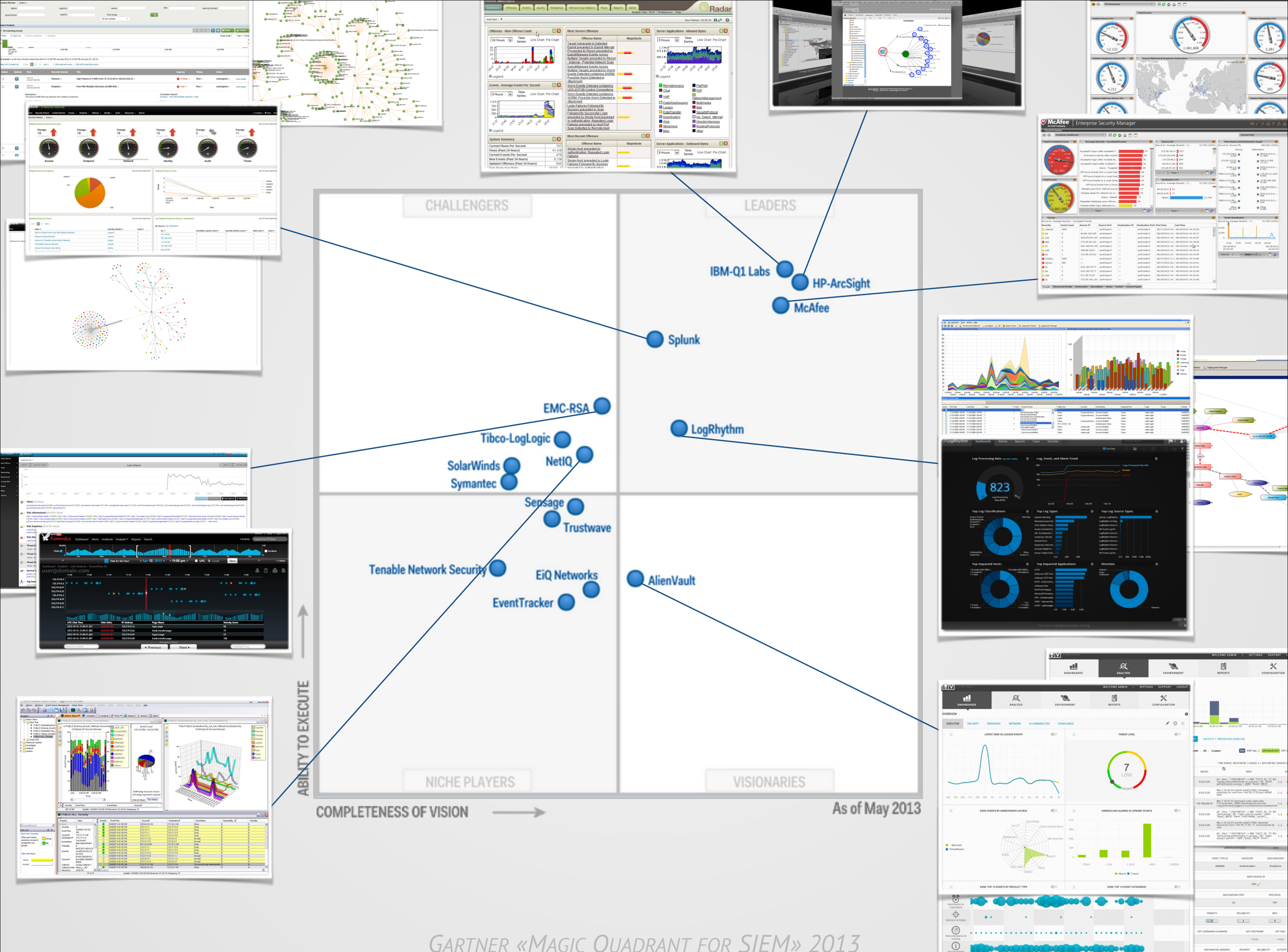
МЕТРИКИ

СКОРОСТЬ ПРИНЯТИЯ РЕШЕНИЙ
КОЛИЧЕСТВО «ОШИБОК»

ЛИШНИЕ ДЕЙСТВИЯ

ОШИБКИ ПЕРВОГО
И ВТОРОГО РОДА

НЕОПТИМАЛЬНЫЙ ПОРЯДОК
РАЗБОРА ИНЦИДЕНТОВ



GARTNER «MAGIC QUADRANT FOR SIEM» 2013

НЕ ОРИЕНТИРОВАНЫ НА ОПЕРАТОРА

ТОЛЬКО ВОЗМОЖНОСТИ

НО ВЕДЬ

МОНИТОРИНГ БЕЗОПАСНОСТИ

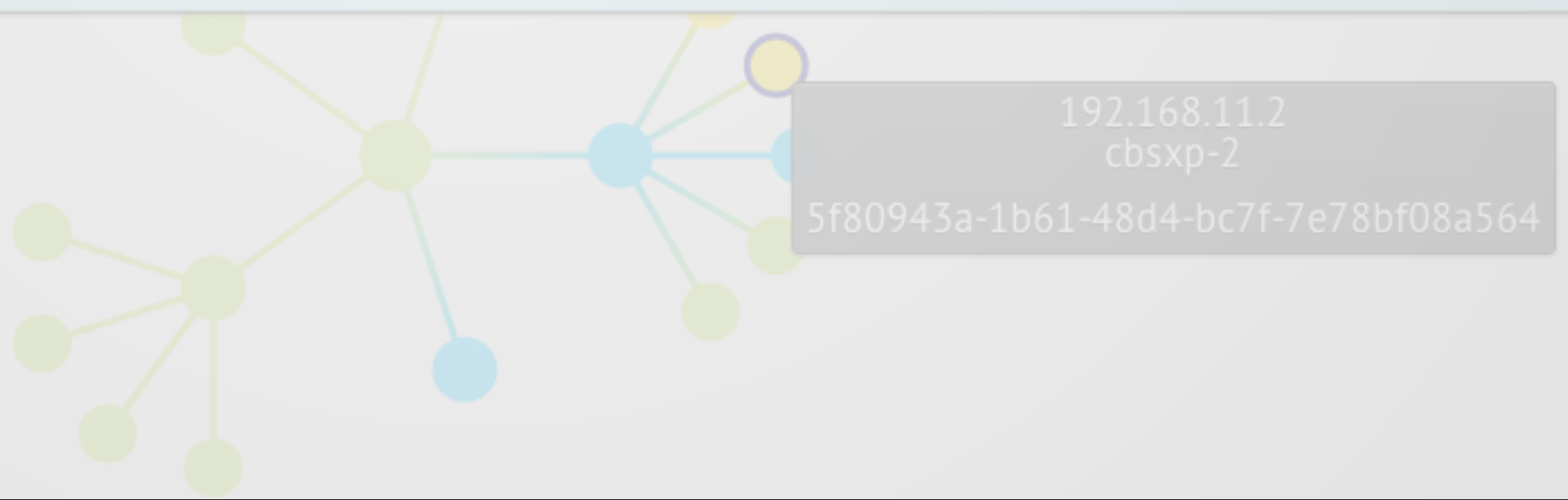
ИМЕННО ТА ОБЛАСТЬ, ГДЕ

ЭФФЕКТИВНОСТЬ ВЗАИМОДЕЙСТВИЯ ОСОБЕННО ВАЖНА

мя	Уровень опасности ▼	IP-адрес	СЗИ	Инфо	Имя компьютера
16:39:12	normal	192.168.11.2	QP	[Warning at 30.01.2014 12:39:12]	cbsxp-2
15:35:30	normal	192.168.11.3	QP	[Warning at 30.01.2014 11:35:30]	cbsxp-3
15:02:24	normal	192.168.11.2	QP	[Warning at 30.01.2014 11:02:24]	cbsxp-2
18:24:46	info	172.16.0.149	Антивирус Касперского 6.0	почтовое вложение [From:"РогочийР.В."] [Subject:Fwd: RE: по АСЗИ ФЭУ-2][Time:2014/01/22 15:23:43]/1.eml/!!! АСЗИ ФЭУ 2 - расчет стоимости корректировка.rar/!!! АСЗИ ФЭУ 2 - расчет стоимости	ARM14

ЧТО ПРЕДЛАГАЕМ МЫ

16:11:07	info	172.16.0.147	Антивирус Касперского 6.0	Обновление завершено успешно	ARM14
16:02:45	info	172.16.0.148	Антивирус Касперского 6.0	Обновление завершено успешно	ARM13
14:11:51	info	172.16.0.147	Антивирус Касперского 6.0	Обновление завершено успешно	ARM14



Время	Уровень опасности ▼	IP-адрес	СЗИ	Инфо	Имя компьютера
2014/03/19 15:57:55	critical	192.168.42.128	Windows Events Log	Завершение работы службы	emb-virtual
2014/03/12 23:00:36	info	172.16.0.56	Windows Events Log	Выход из системы	ARM7
2014/03/19 16:28:39	info	172.16.0.56	Windows Events Log	Вход в систему	ARM7
2014/03/19 16:27:44	info	172.16.0.56	Windows Events Log	Выход из системы	ARM7
2014/03/19 16:27:39	info	172.16.0.56	Windows Events Log	Выход из системы	ARM7

AJAX

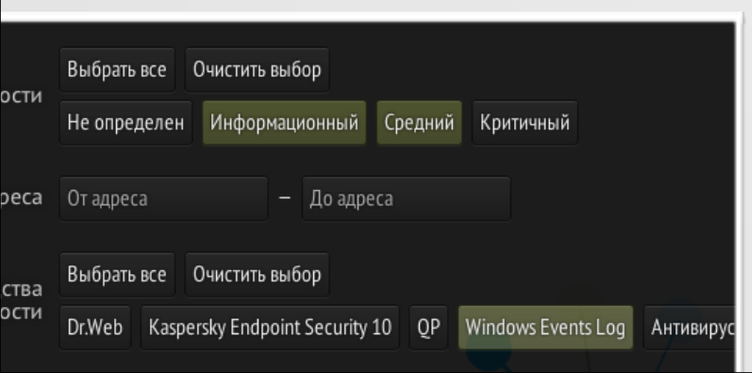
ОДНА СТРАНИЦА

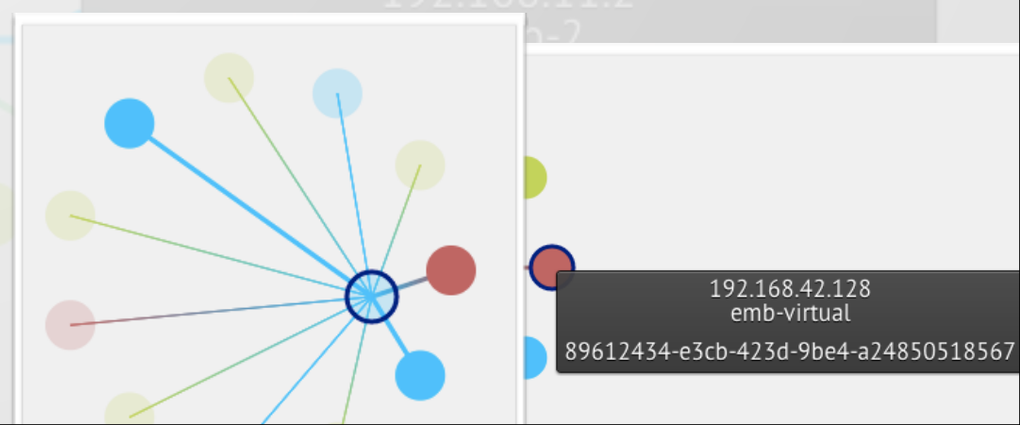
БЕСКОНЕЧНЫЙ СКРОЛЛИНГ В ТАБЛИЦАХ

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ ДАННЫХ

ДИНАМИЧЕСКАЯ КАРТА СЕТИ

СВЯЗНЫЙ ГРАФ ВСЕХ ДАННЫХ





Время	Уровень опасности ▼	IP-адрес	СЗИ	Инфо	Имя компьютера
2014/03/19 15:57:55	critical	192.168.42.128	Windows Events Log	Завершение работы службы	emb-virtual
2014/03/12 23:00:36	info	172.16.0.56	Windows Events Log	Выход из системы	ARM7
2014/03/19 16:28:39	info	172.16.0.56	Windows Events Log	Вход в систему	ARM7
2014/03/19 16:27:44	info	172.16.0.56	Windows Events Log	Выход из системы	ARM7
2014/03/19 16:27:39	info	172.16.0.56	Windows Events Log	Выход из системы	ARM7

AJAX

ОДНА СТРАНИЦА

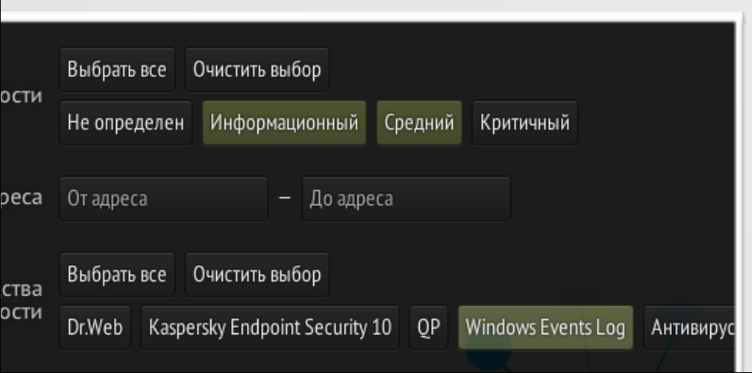
БЕСКОНЕЧНЫЙ СКРОЛЛИНГ В ТАБЛИЦАХ

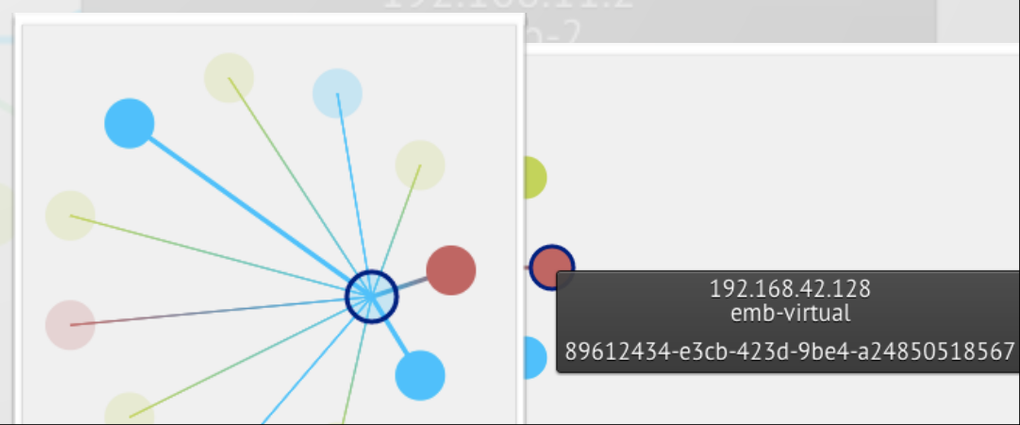
АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ ДАННЫХ

ДИНАМИЧЕСКАЯ КАРТА СЕТИ

СВЯЗНЫЙ ГРАФ ВСЕХ ДАННЫХ

+ АДАПТАЦИЯ НАГРУЗКИ НА ОПЕРАТОРА





ОБРАТИМСЯ К

КОГНИТИВИСТИКЕ

СНИЖЕНИЕ РАБОТОСПОСОБНОСТИ

СОСТОЯНИЯ

МОНОТОНИЯ и **УСТАЛОСТЬ**

НЕДОСТАТОЧНАЯ НАГРУЗКА

ПЕРЕГРУЗКА

Леонова, Величковская «Дифференциальная диагностика состояний сниженной работоспособности» 2002

Ильин «Психофизиология состояний человека» 2005

СНИЖЕНИЕ РАБОТОСПОСОБНОСТИ

ФАКТОРЫ

ПРОДОЛЖИТЕЛЬНОСТЬ РАБОТЫ

УДЕРЖАНИЕ ВНИМАНИЯ

ТРУДОЗАТРАТЫ vs **РЕЗУЛЬТАТ**

СЛОЖНОСТЬ ЗАДАЧИ

ФИЗИЧЕСКОЕ СОСТОЯНИЕ

МОТИВАЦИЯ

Kato, Endo et al. «Mental fatigue and impaired response processes: event-related brain potentials in a Go/NoGo task» 2009

Williamson, Lombardi et al. «The link between fatigue and safety» 2011

Дорохов «Сомнология и безопасность профессиональной деятельности» 2013

СЛОЖНАЯ ЗАДАЧА

БОЛЬШОЕ КОЛИЧЕСТВО
ЦЕЛЕЙ / ЭЛЕМЕНТОВ / СВЯЗЕЙ

ИЗМЕНЯЕТСЯ со **ВРЕМЕНЕМ**

НЕ ПРОГНОЗИРУЕМА

ОГРАНИЧЕНА по **ВРЕМЕНИ**

Dörner, Kreuzig et al. «Lohhausen: Vom Umgang mit Unbestimmtheit und Komplexität» 1983
Funke «Complex problem solving: A case for complex cognition?» 2010

СНИЖЕННАЯ РАБОТОСПОСОБНОСТИ

УХУДШАЕТ **ВНИМАНИЕ**

УХУДШАЕТ **РЕАКЦИИ** НА **СТИМУЛЫ**

УВЕЛИЧИВАЕТ **ЧИСЛО ОШИБОК**

УХУДШАЕТ **ВОСПРИЯТИЕ СОБСТВЕННОЙ ЭФФЕКТИВНОСТИ**

Boksem, Meijman et al. «Effects of mental fatigue on attention: An ERP study» 2005

Lorist, Boksem et al. «Impaired cognitive control and reduced cingulate activity during mental fatigue» 2005

ОПЕРАТОР БУДЕТ УСТАВАТЬ

ЕГО ЭФФЕКТИВНОСТЬ БУДЕТ СНИЖАТЬСЯ

ОПЕРАТОР БУДЕТ УСТАВАТЬ

ЕГО ЭФФЕКТИВНОСТЬ БУДЕТ СНИЖАТЬСЯ

НО ЧТО, ЕСЛИ...

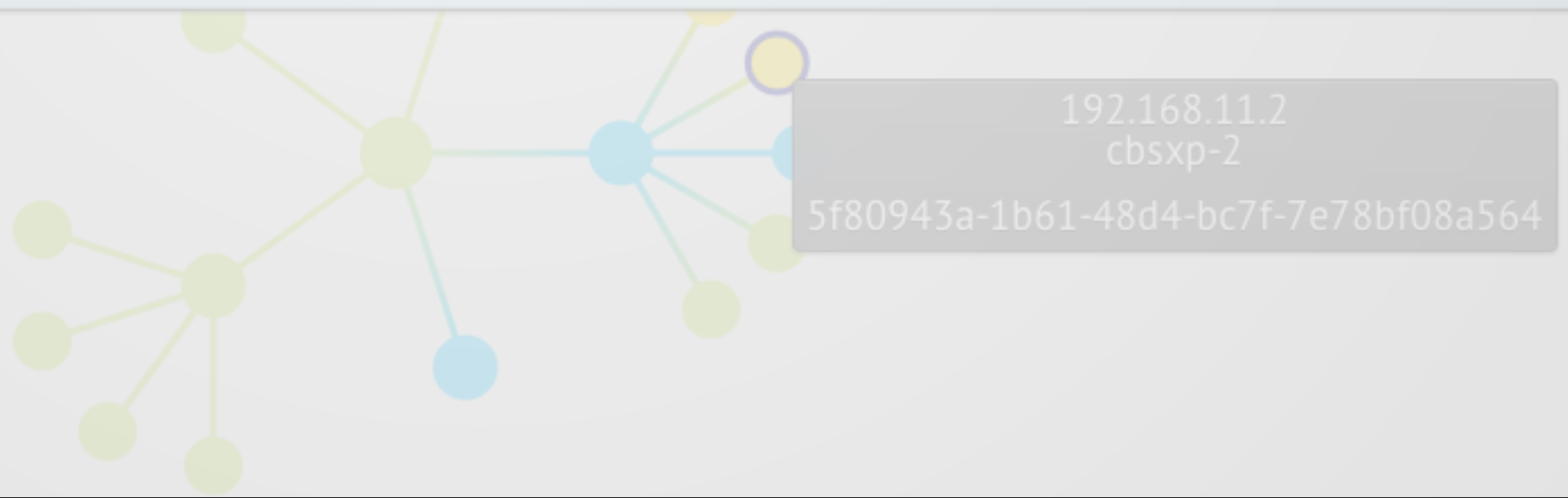
МЫ МОЖЕМ ЕМУ ПОМОЧЬ

СДЕЛАВ ЕГО РАБОТУ В ТЕЧЕНИЕ ДНЯ ЭФФЕКТИВНЕЕ

мя	Уровень опасности ▼	IP-адрес	СЗИ	Инфо	Имя компьютера
16:39:12	normal	192.168.11.2	QP	[Warning at 30.01.2014 12:39:12]	cbsxp-2
15:35:30	normal	192.168.11.3	QP	[Warning at 30.01.2014 11:35:30]	cbsxp-3
15:02:24	normal	192.168.11.2	QP	[Warning at 30.01.2014 11:02:24]	cbsxp-2
18:24:46	info	172.16.0.149	Антивирус Касперского 6.0	почтовое вложение [From:"РогочийР.В."] [Subject:Fwd: RE: по АСЗИ ФЭУ-2][Time:2014/01/22 15:23:43]/1.eml/!!! АСЗИ ФЭУ 2 - расчет стоимости корректировка.rar/!!! АСЗИ ФЭУ 2 - расчет стоимости	ARM14

НАШИ ГИПОТЕЗЫ

16:11:07	info	172.16.0.147	Антивирус Касперского 6.0	Обновление завершено успешно	ARM14
16:02:45	info	172.16.0.148	Антивирус Касперского 6.0	Обновление завершено успешно	ARM13
14:11:51	info	172.16.0.147	Антивирус Касперского 6.0	Обновление завершено успешно	ARM14



ПРЕДЕЛ КОГНИТИВНЫХ ВОЗМОЖНОСТЕЙ

ДОСТИГАЕТСЯ ОПЕРАТОРОМ ВО ВРЕМЯ РАБОТЫ

МЕНЯЕТСЯ В ТЕЧЕНИЕ ДНЯ

ПАРАМЕТРЫ ВЗАИМОДЕЙСТВИЯ

МЕНЯЮТСЯ В ТЕЧЕНИЕ ДНЯ

ОЦЕНИВАЮТ ПРЕДЕЛ ВОЗМОЖНОСТЕЙ ОПЕРАТОРА

ЭФФЕКТИВНОСТЬ РАБОТЫ ОПЕРАТОРА

ПОВЫШАЕТСЯ ПРИ АДАПТАЦИИ ИНТЕРФЕЙСА ПОД ПРЕДЕЛ

СНИЖАЕТСЯ ПРИ ПРЕВЫШЕНИИ ПРЕДЕЛА

РЕАКЦИЯ

ВОСПРИЯТИЕ

РАБОЧАЯ ПАМЯТЬ

ДОЛГОСРОЧНАЯ ПАМЯТЬ

КОГНИТИВНЫЕ ХАРАКТЕРИСТИКИ

РАСПОЗНАВАНИЕ ОБРАЗОВ

КОГНИТИВНАЯ НАГРУЗКА

ВНИМАНИЕ

РЕШЕНИЕ ЗАДАЧ

t_r реакции – t_{cs} сложного стимула – Δ_{sr} простой реакции

ВОСПРИЯТИЕ

t_{sr} реакции – t_{ss} простого стимула

РЕАКЦИЯ

N_{wm} повторных обращений к ранее отображенной информации

РАБОЧАЯ ПАМЯТЬ

N_m обращений к подсказкам об интерфейсе

ДОЛГОСРОЧНАЯ ПАМЯТЬ

ХАРАКТЕРИСТИКИ ВЗАИМОДЕЙСТВИЯ

РАСПОЗНАВАНИЕ ОБРАЗОВ

C_v предпочтения в методах отображения

КОГНИТИВНАЯ НАГРУЗКА

$$L(p(t_r, t_{cs}, \Delta_{sr}),\ N_{wm},\ a(N_r, N_w),\ r(t_{is}, t_{ir}, \Delta_{st}))$$

ВНИМАНИЕ

$$\frac{N_r \text{ правильных действий} - N_w \text{ неправильных}}{N_r + N_w}$$

РЕШЕНИЕ ЗАДАЧ

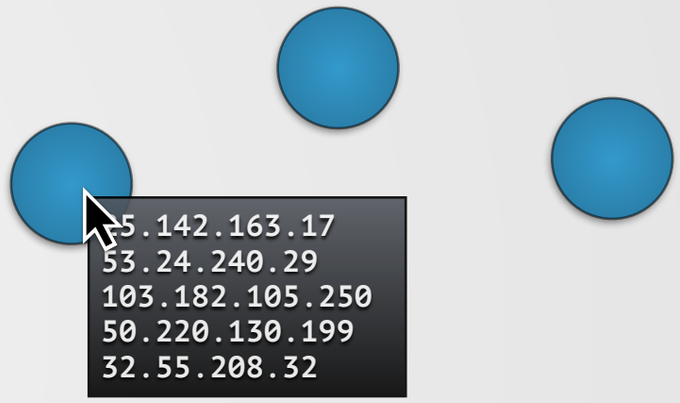
$$\frac{\Delta_r \text{ решения инцидента}}{\Delta_{st} \text{ стандартное для такого инцидента}}$$

НАЧАЛЬНЫЕ ЗАМЕРЫ

РЕАКЦИЯ

t_{sr} реакции — t_{ss} простого стимула

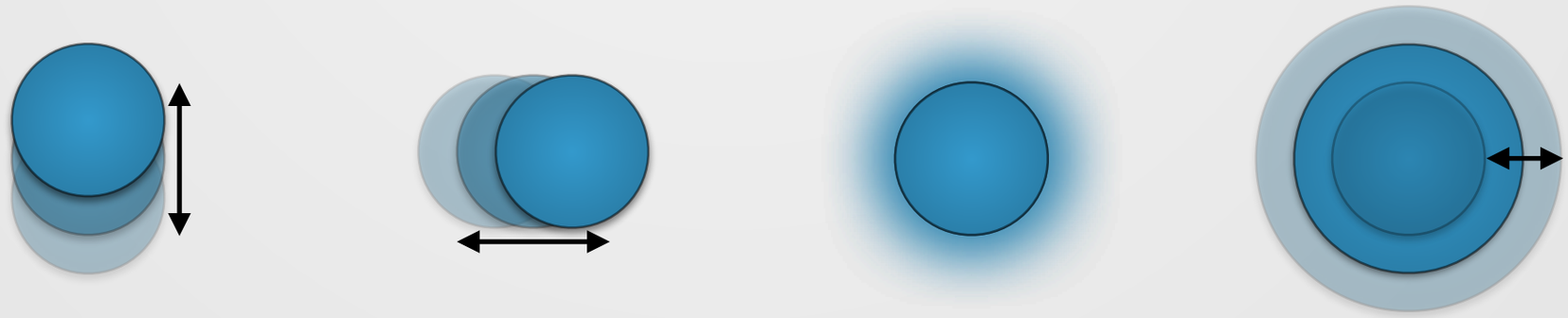
ВОСПРИЯТИЕ + РАБОЧАЯ ПАМЯТЬ



t_r реакции — t_{cs} сложного стимула — Δ_{sr} простой реакции

N_h скрытых объектов, N_g групп объектов

РАСПОЗНАВАНИЕ ОБРАЗОВ



Donders «On the speed of mental processes» 1868

Dutta et al. «Evaluating benefits and distractions of animated secondary displays for attention-centric primary tasks» 2002

ВО ВРЕМЯ МОНИТОРИНГА

ВОСПРИЯТИЕ t_r реакции $-$ t_{cs} сложного стимула $-$ Δ_{sp} стандартной реакции для такой нагрузки

ВНИМАНИЕ

$$\frac{N_r \text{ правильных действий} - N_w \text{ неправильных}}{N_r + N_w}$$

РАБОЧАЯ ПАМЯТЬ N_{wm} повторных обращений к ранее отображенной информации

РЕШЕНИЕ ЗАДАЧ

$$\frac{\Delta_r \text{ решения инцидента}}{\Delta_{st} \text{ стандартное для такого инцидента}}$$

ДОЛГОСРОЧНАЯ ПАМЯТЬ N_m обращений к подсказкам об интерфейсе

АДАПТАЦИЯ КОГНИТИВНОЙ НАГРУЗКИ

$$L(p(t_r, t_{cs}, \Delta_{sp}),\ N_{wm},\ a(N_r, N_w),\ r(t_{is}, t_{ir}, \Delta_{st}))$$

- $p(t_r, t_{cs}, \Delta_{sp})$ — ВОСПРИЯТИЕ
- N_{wm} — РАБОЧАЯ ПАМЯТЬ
- $a(N_r, N_w)$ — ВНИМАНИЕ
- $r(t_{is}, t_{ir}, \Delta_{st})$ — РЕШЕНИЕ ЗАДАЧ

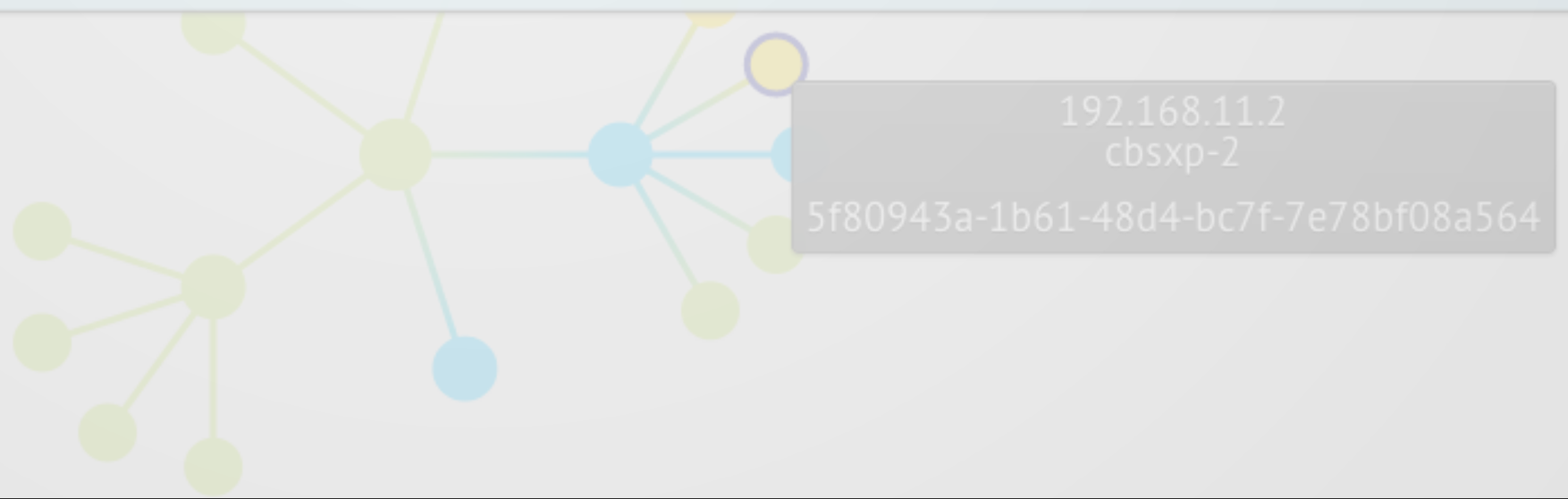
ВАЖНОСТЬ СОБЫТИЯ — $I_e(S_e, u(t_e), I_h)$

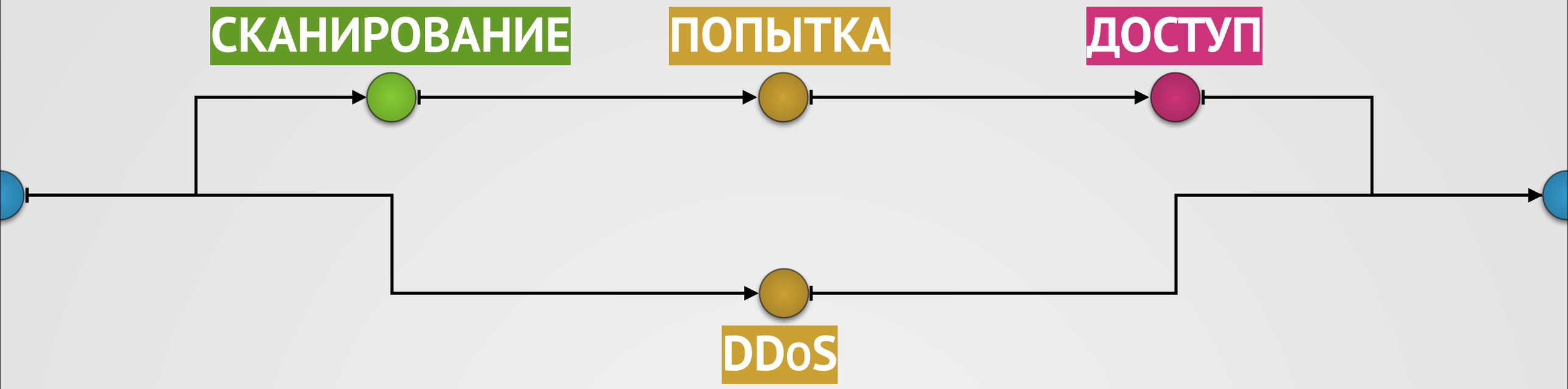
- S_e — ОПАСНОСТЬ
- $u(t_e)$ — АКТУАЛЬНОСТЬ
- I_h — ВАЖНОСТЬ УЗЛА

мя	Уровень опасности ▼	IP-адрес	СЗИ	Инфо	Имя компьютера
16:39:12	normal	192.168.11.2	QP	[Warning at 30.01.2014 12:39:12]	cbsxp-2
15:35:30	normal	192.168.11.3	QP	[Warning at 30.01.2014 11:35:30]	cbsxp-3
15:02:24	normal	192.168.11.2	QP	[Warning at 30.01.2014 11:02:24]	cbsxp-2
18:24:46	info	172.16.0.149	Антивирус Касперского 6.0	почтовое вложение [From:"РогочийР.В."] [Subject:Fwd: RE: по АСЗИ ФЭУ-2][Time:2014/01/22 15:23:43]/1.eml/!!! АСЗИ ФЭУ 2 - расчет стоимости корректировка.rar/!!! АСЗИ ФЭУ 2 - расчет стоимости	ARM14

ТЕСТИРОВАНИЕ

16:11:07	info	172.16.0.147	Антивирус Касперского 6.0	Обновление завершено успешно	ARM14
16:02:45	info	172.16.0.148	Антивирус Касперского 6.0	Обновление завершено успешно	ARM13
14:11:51	info	172.16.0.147	Антивирус Касперского 6.0	Обновление завершено успешно	ARM14





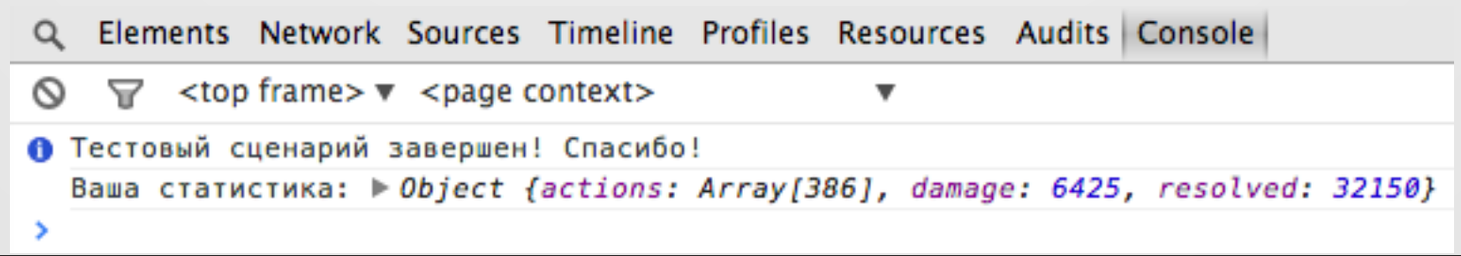
МОДЕЛЬ УЩЕРБА

ЗА **АТАКУ** 10–1000 ЕД. УРОНА

ЗА 10 СЕКУНД **ПРОСТОЯ** 1–100 ЕД. УРОНА

ЦЕЛЬ

МИНИМИЗИРОВАТЬ ПОТЕРИ ЗА 25 МИНУТ



ИНТЕРФЕЙСЫ СОИБ НЕЭФФЕКТИВНЫ

ОПЕРАТОР — «БУТЫЛОЧНОЕ ГОРЛЫШКО» СОИБ

ПРОИЗВОДИТЕЛЬНОСТЬ ОПЕРАТОРА СНИЖАЕТСЯ

МОЖНО УПРАВЛЯТЬ НАГРУЗКОЙ НА ОПЕРАТОРА

АДАПТАЦИЯ КОГНИТИВНОЙ НАГРУЗКИ ПОВЫШАЕТ ЭФФЕКТИВНОСТЬ ОПЕРАТОРА

МОЖНО ОПРЕДЕЛЯТЬ УРОВЕНЬ ЗАГРУЖЕННОСТИ ОПЕРАТОРА

ПО ХАРАКТЕРИСТИКАМ ЕГО ВЗАИМОДЕЙСТВИЯ С ИНТЕРФЕЙСОМ

Спасибо за внимание!

http://tolya.github.io/interview-ru.html

tolya@lvk.cs.msu.su

gamajun@seclab.cs.msu.su

Елизаров А.В.

к.ф.-м.н., с.н.с., заведующий лабораторией Гамаюнов Д.Ю.

МГУ

Лаборатория Безопасности Информационных Систем

INFORMATION SYSTEMS SECURITY LAB

ВМиК