
# SOC
# Как не проиграть войну?

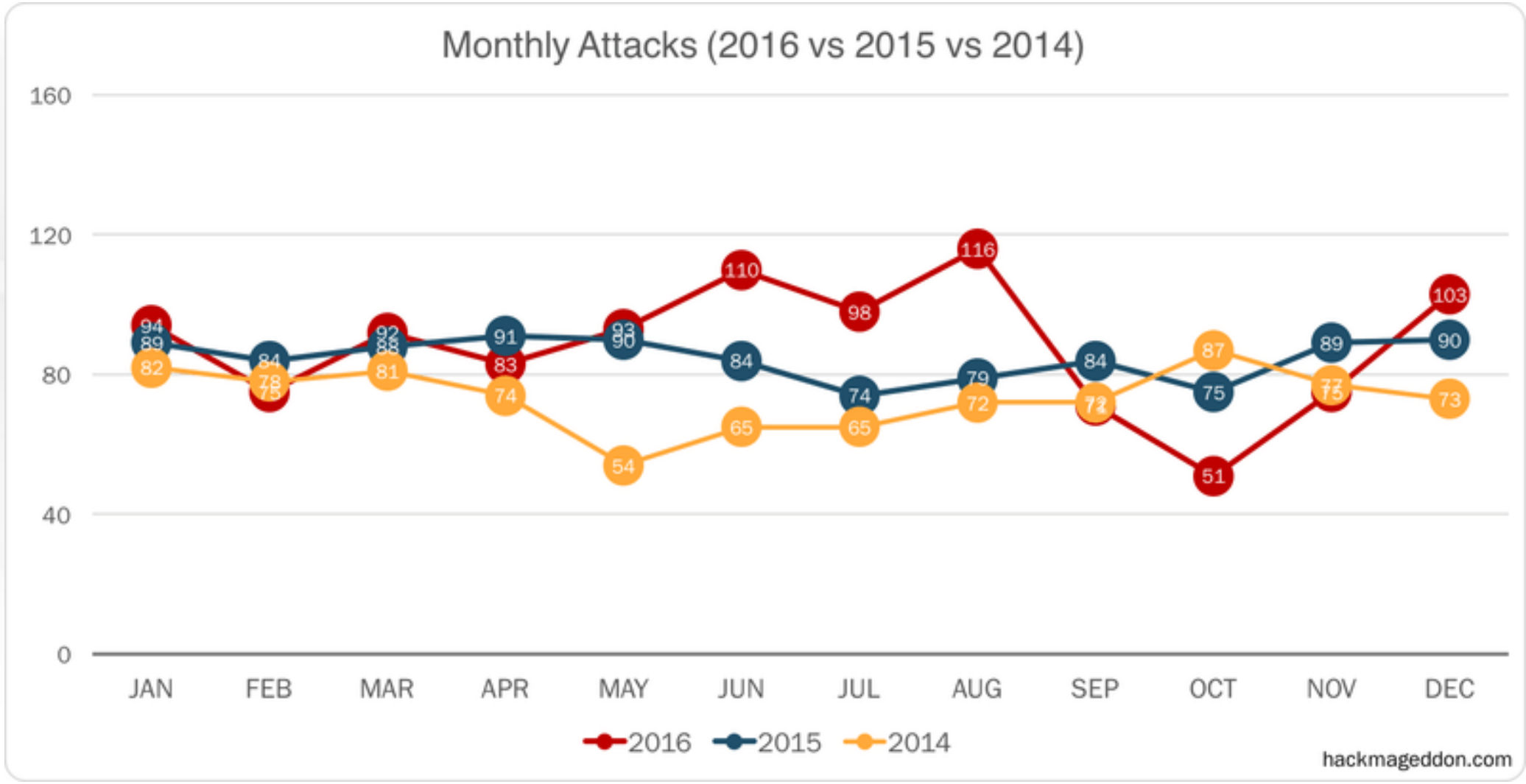
Алексей МАЛЬНЕВ,

Заместитель директора департамента ИБ АМТ-ГРУП amalnev@amt.ru

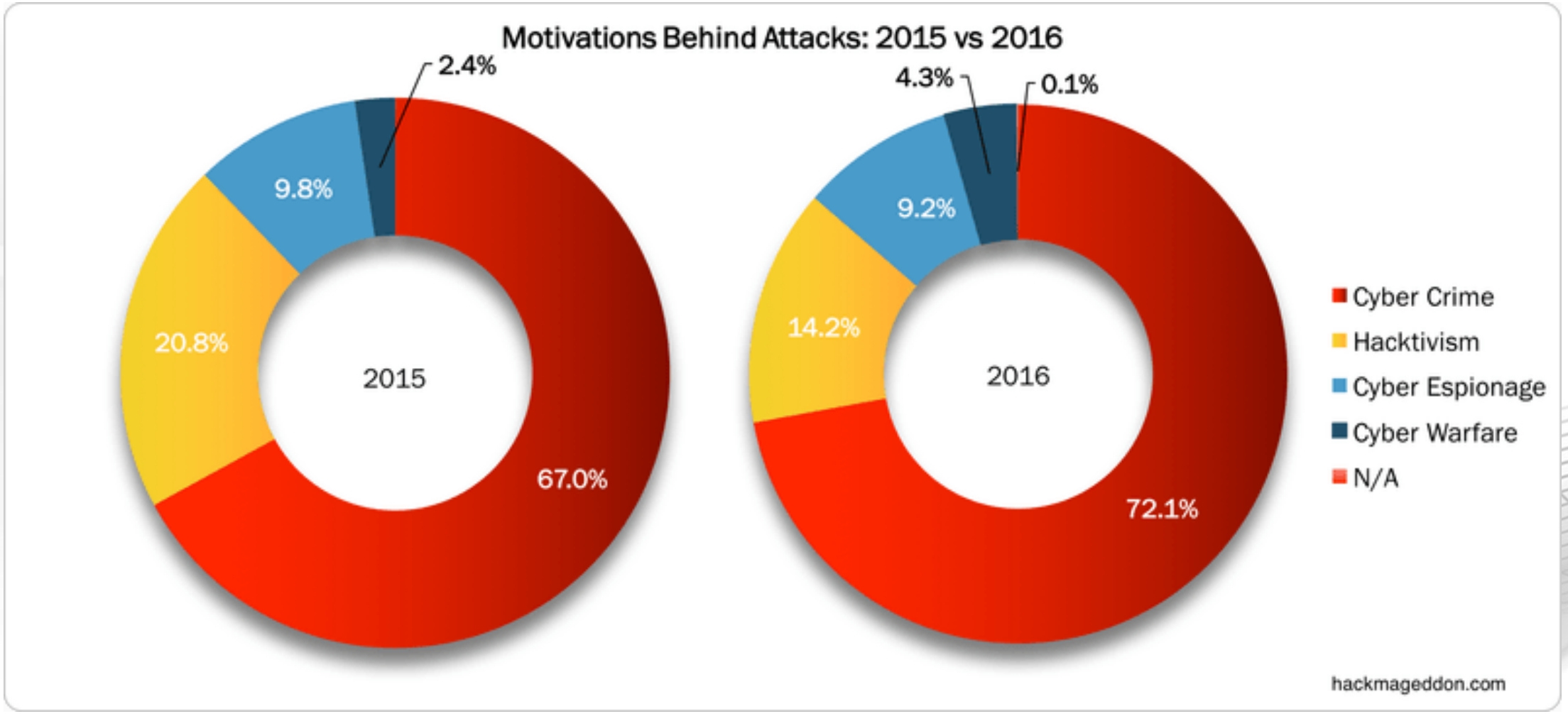
# Угрозы нового типа для финансового сектора

AMT GROUP

# Критичные инциденты



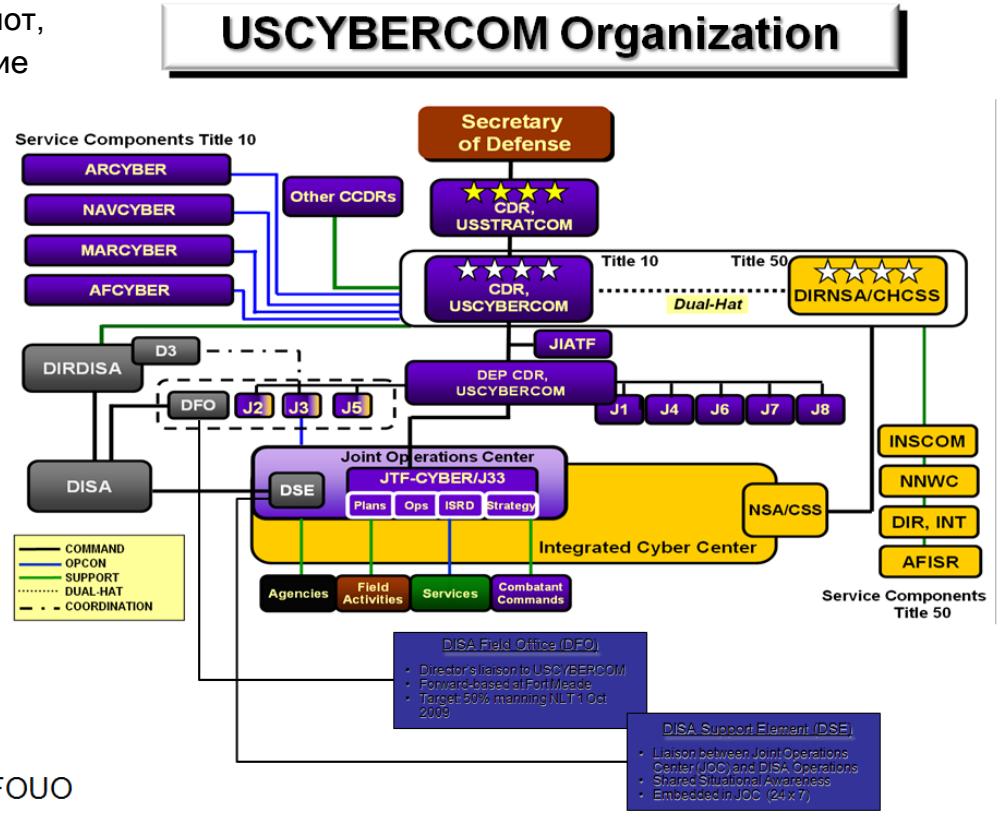
# Мотивация злоумышленника



# Источники угроз
# Пример Cyber Warfare

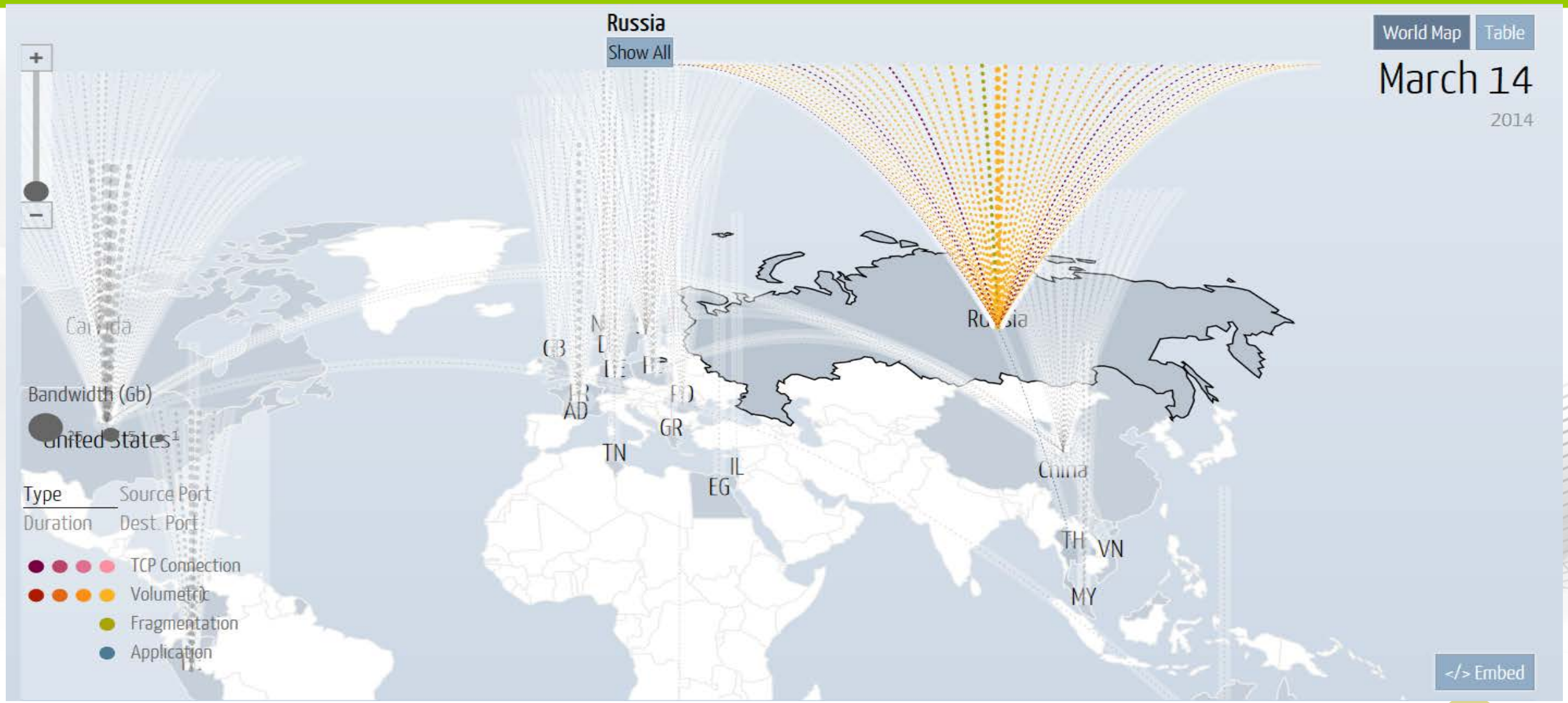


- Расположено на территории военной базы Форт-Мид, штат Мэриленд
- Функционирует с 21 мая 2010 года
- Объединило ранее созданные организации (Соединение глобальных сетевых операций JTF-GNO и командование сетевой войны JFCC-NW и тд)
- Включает: 9-е армейское командование связи, 10 флот, 24 воздушная армия и кибернетическое командование корпуса морской пехоты
- 6 апреля 2016 года: МО Эштон Картер дал первое задание военного времени: атаковать ИГ с целью нарушения руководства ИГ




FOUO

# “Волатильность” на российском рынке




http://www.digitalattackmap.com/

# “Волатильность” на российском рынке



14 марта 2014

AMT GROUP

# “Волатильность” на российском рынке

**Октябрь-декабрь 2013:**
Атакован сайт партии Украины “Батьківщина
**Атакован Сайт Центробанка России**
**Январь-Февраль 2014:**
**Атакованы информационные системы сайта почты России**
**Атакован сайт “Ведомостей”**
**Март 2014:**
**Атакован официальный сайт главы России (kremlin.ru)**
**Атакованы крымские сайты референдума (referendum2014.org.ua)**
**Ряд форумов Севастополя и Крыма**
**Атакован сайт Банка России**
**Атакован сайт МИД России**
**Атакован сайт Альфабанка**
**Атакован сайт ВТБ24**
**Атакованы российские биржевые площадки**
**Атакованы сети передачи данных провайдеров Интернет в России**
Атакован сайт NATO Cooperative Cyber Defense Center of Excellence (CCDCOE)
Атакован сайт украинского информагентства УНИАН
**Атакован сайт Верховного Совета Крыма**
**Атакован сайт ТКС Банка**
**Апрель 2014:**
**Атакован сайт “МК”**
**Атакован сайт Russia Today**
**Атакован сайт “Новой Газеты”**
**Май 2014:**
Атакован сайт информационного агентства "Украинские национальные новости"
**Атакован сайт “Известий”**
Атакован сайт ЦИК Украины


40%

40%

10%

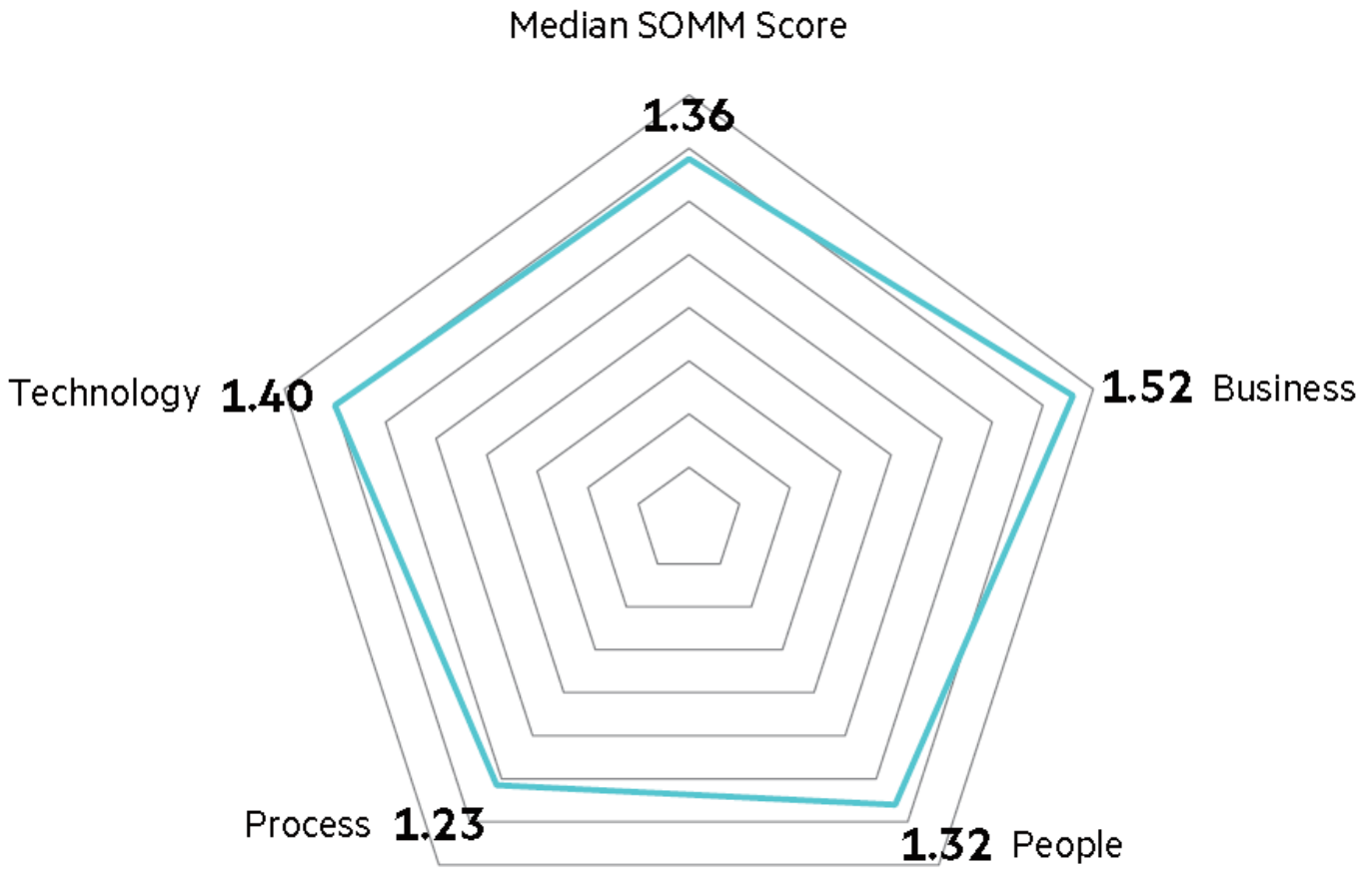
AMT GROUP

# Обзор методик оценки зрелости SOC

AMT GROUP

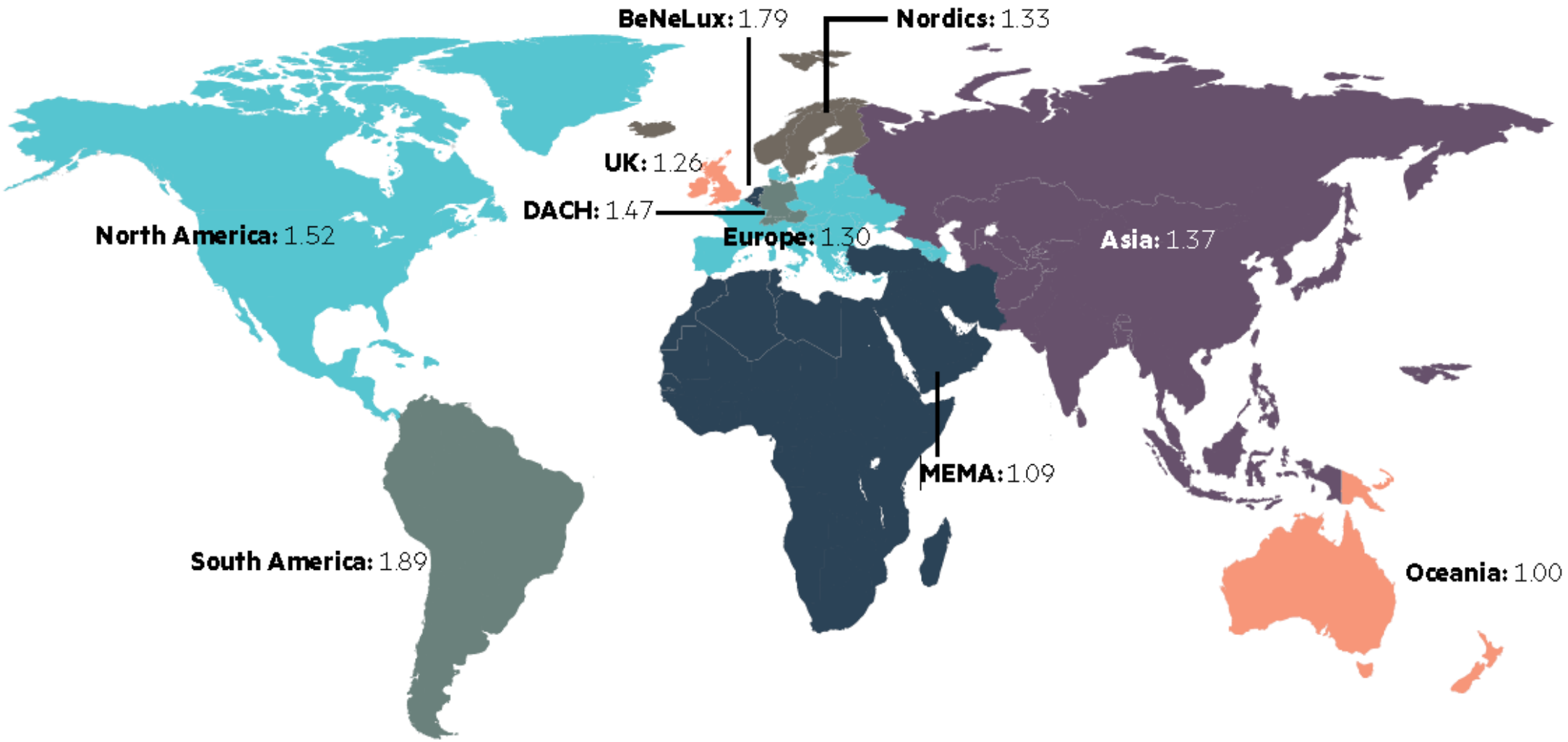
# Методики оценки зрелости SOC
# Security Operations Maturity Model (SOMM)

| Уровень SOMM | Оценка | Описание функций |
|---|---|---|
| Level 0 | Incomplete | Не реализованы |
| Level 1 | Initial | От случая к случаю |
| Level 2 | Managed | Повторяемые |
| Level 3 | Defined | Субъективно выполняются |
| Level 4 | Measured | Объективно выполняются (измеряются) |
| Level 5 | Optimizing | Избыточны |

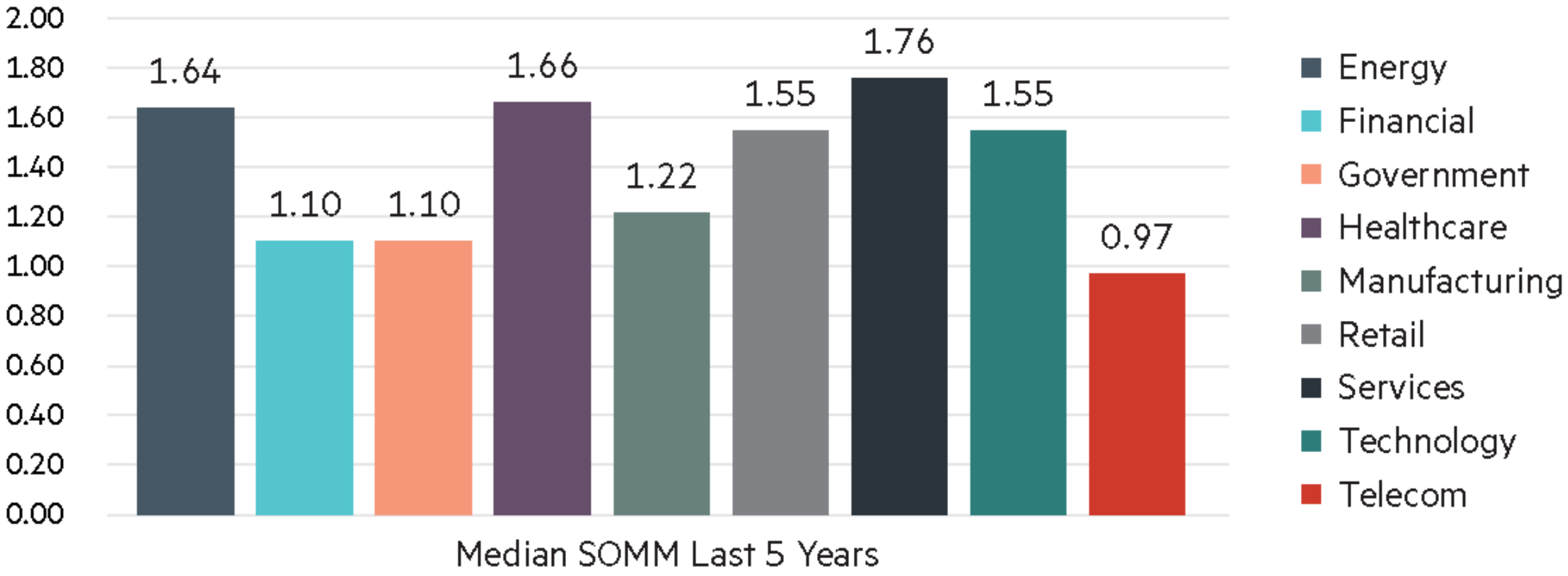



Carnegie Mellon Software Engineering
Institute Capability Maturity Model for Integration (SEI-CMMI))

# Методики оценки зрелости SOC
# Security Operations Maturity Model (SOMM)



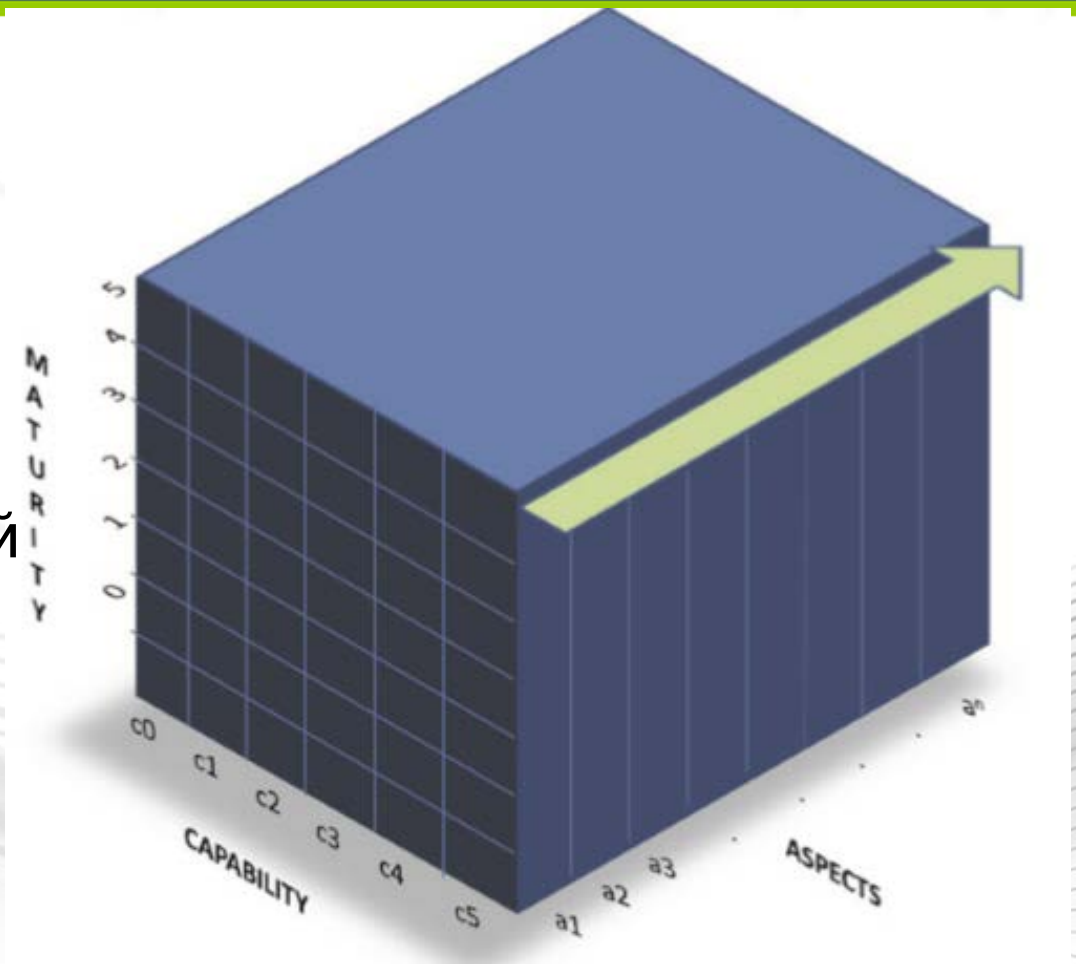
# Методики оценки зрелости SOC
# Security Operations Maturity Model (SOMM)




AMT GROUP

# Методики оценки зрелости SOC MSSP Rhodes University

- **Maturity** (зрелость процессов/функций SOC)
- **Aspect** (функциональность процессов/функций SOC)
- **Capability** (глубина/степень реализации процессов/функций SOC)



# Методики оценки зрелости SOC MSSP
# Rhodes University. Оценка зрелости процессов

| Модель зрелости | Описание уровней | Примечание |
|---|---|---|
| NIST CSEAT IT SMM | 1. Policy<br>2. Procedure<br>3. Implementation<br>4. Testing<br>5. Integration | Фокус на уровень документирования операций |
| Citigroup Information Security Evaluation Model (CITI-ISEM) | 1. Complacency<br>2. Acknowledgment<br>3. Integration<br>4. Common Practice<br>5. Continuous Improvement | Фокус на осведомленность |
| CobiT, ITIL, Maturity Model | 1. Initial/ad-hoc<br>2. Repeatable but intuitive<br>3. Defined process<br>4. Managed and measured<br>5. Optimized | Фокус на аудит специфичных процедур |
| SSE-CMM Model | 1. Performed informally<br>2. Planned and tracked<br>3. Well-defined<br>4. Quantitatively controlled<br>5. Continuously improving | Фокус на ИБ инженерию и ПО |
| CERT/CSO Security Capability Assessment | 1. Exists<br>2. Repeatable<br>3. Designed Person<br>4. Documented<br>5. Reviewed and updated | Фокус на измеримость и качество документирования |

# Методики оценки зрелости SOC MSSP
## Rhodes University. Оценка зрелости процессов

| Модель зрелости | Описание уровней | Примечание |
|---|---|---|
| 0 | **Non Existent** | Cobit 0 |
| 1 | **Initial** | CoBIT, SSE, ITIL: Initial CERT: Exists |
| 2 | **Repeatable** | (CoBIT, ITIL, SSECMM and CERT/CSO) |
| 3 | **Defined Process** | (CERT/CSO) / Well Defined (SSECMM), Defined Process (CoBIT), Common Practice (CITI-ISEM |
| 4 | **Reviewed and updated** | CERT/CSO), Quantitatively controlled (SSECMM), Managed and Measureable (CoBIT) and Continuous Improvement (CITIISEM) |
| 5 | **Continuously Optimized** | Optimised (CoBIT), Continuously Improving (CITIISEM), Continuously Improving (SSECMM) |

# Методики оценки зрелости SOC MSSP
# Rhodes University. Аспекты (функции) и Capability (реализация функций)

## Aspects

**Первичные аспекты/функции:**

- Log Collection
- Log Retention and Archival
- Log Analysis
- Monitoring of Security Environments for Security Events.
- Diversity of devices integrated
- Incident Management
- Reaction to threats
- Threat Identification
- Reporting

**Вторичные аспекты/функции**

- Malware analysis
- Vulnerability Scanning
- Vulnerability Analysis
- Device Management
- Identity Attestation and Recertification
- Penetration testing
- Type of Industry verticals monitored
- Integration with Physical Security controls.

## Capability

Log collection: от негарантированного сбора до 99% гарантии сбора
Log Retention and Archival (от отсутствия архивирования, до N лет хранения)
…….

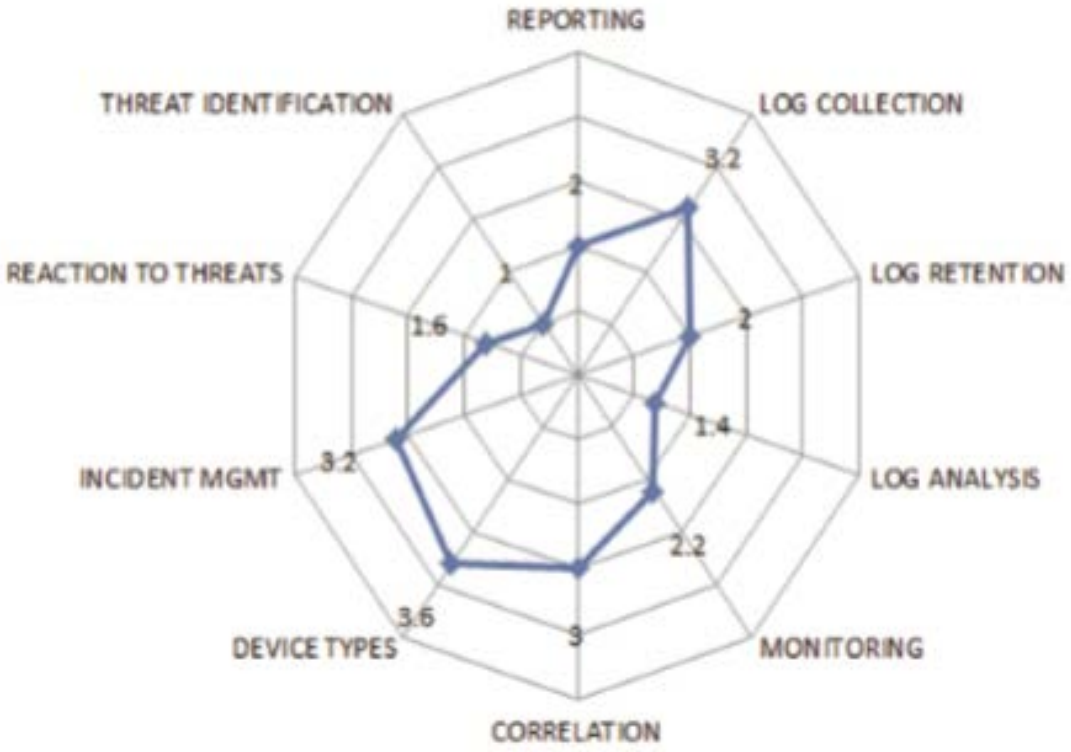
Методологии:
SANS Critical Control (GSEC)
Cisco Systems (How to build SOC)
ISO/IEC 27001:2005 Requirements

AMT GROUP

# Методики оценки зрелости SOC MSSP
# Rhodes University. Пример расчёта SOC Score

| Aspect | Capability | Maturity | Rating |
|---|---|---|---|
| REPORTING | 2 | 2 | 2 |
| LOG COLLECTION | 3.5 | 3 | 3.2 |
| LOG RETENTION | 2 | 2 | 2 |
| LOG ANALYSIS | 2 | 1 | 1.4 |
| MONITORING | 2.5 | 2 | 2.2 |
| CORRELATION | 3 | 3 | 3 |
| DEVICE TYPES | 2 | 4 | 3.6 |
| INCIDENT MGMT | 2 | 4 | 3.2 |
| REACTION TO THREATS | 1 | 2 | 1.6 |
| THREAT IDENTIFICATION | 1 | 1 | 1 |
| **SOC SCORE** | | | 46,4 |

$$S = \frac{\sum_1^n (\alpha C_i + \beta M_i)}{0.05 \times n}$$



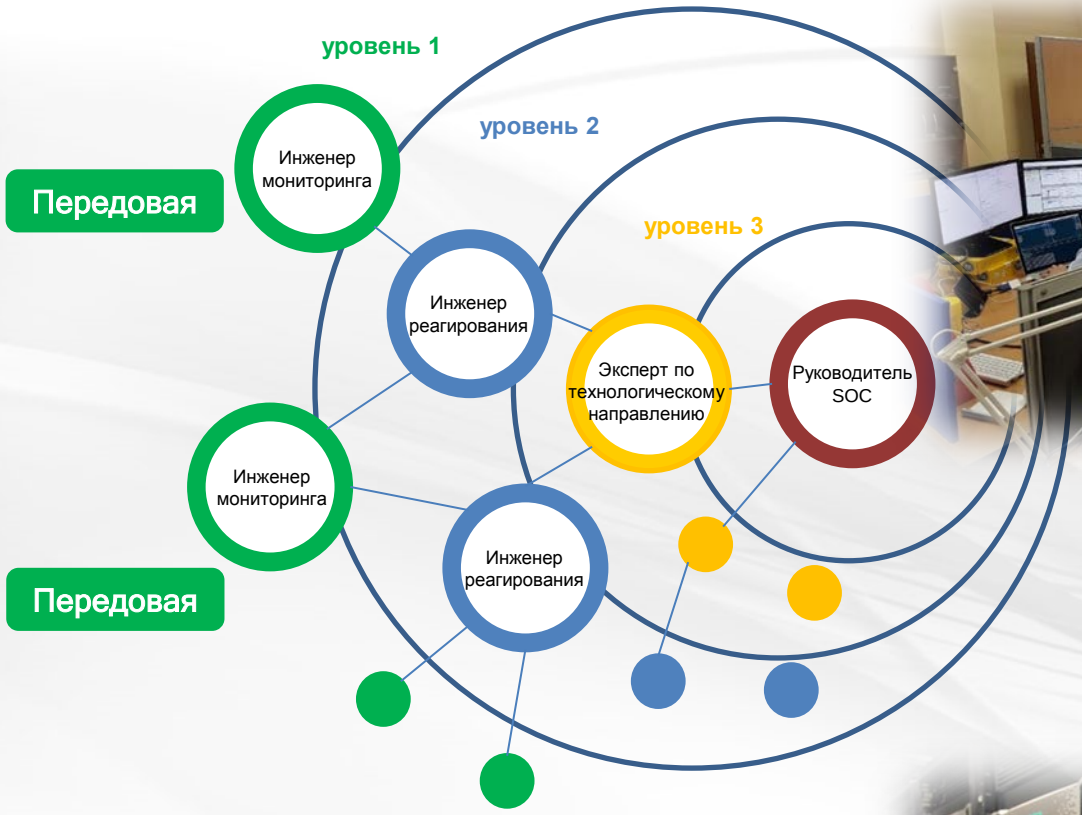

AMT GROUP

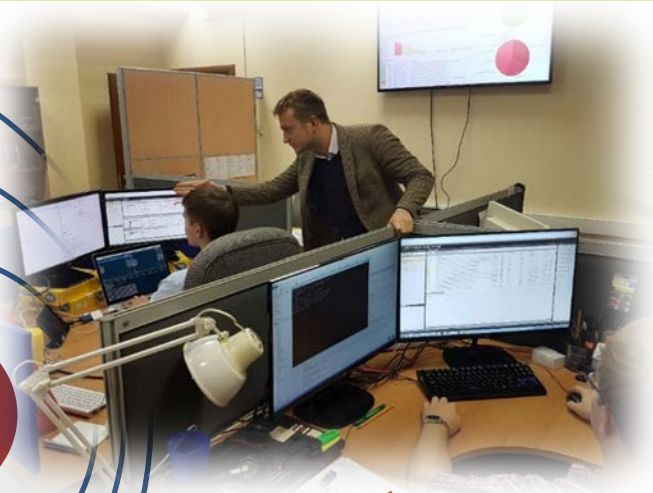
# AMTSOC

AMT GROUP

# Принцип работы сервиса AMTSOC





## Наши эксперты

## Заказчик

## Оборудование

# Позиционирование AMTSOC



# Пример: SLA услуги

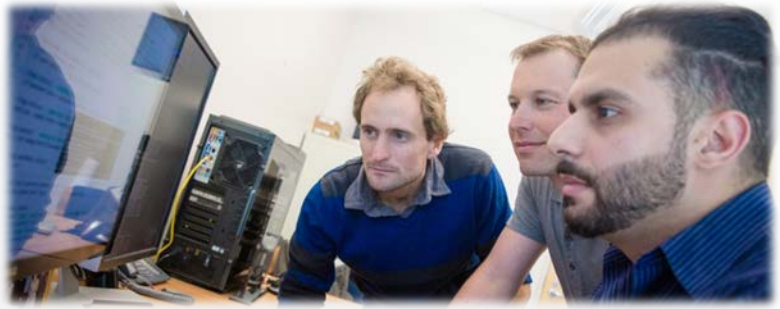



| Парт-номер (AMTSOC SLA) | Режим работы | Состав сервиса | Время реакции | Дежурный инженер |
|---|---|---|---|---|
| **AMTSOC-STD** | 8 x 5 | – Проактивный мониторинг ИБ<br>– Рекомендации, помощь в реагировании;<br>– Ежемесячные отчеты | NBD | Нет |
| **AMTSOC-ADV** | 24 x 7 | – Проактивный мониторинг ИБ<br>– Рекомендации, помощь в реагировании;<br>– Ежемесячные отчеты | 4 часа | 1 уровень |
| **AMTSOC-OUTSRC-STD** | 8 x 5 | – Проактивный мониторинг ИБ<br>– Рекомендации, помощь в реагировании;<br>– Ежемесячные отчеты<br>– **Техническая поддержка оборудования ИБ** | 30 минут | 1-2 уровень |
| **AMTSOC-OUTSRC-ADV** | 24 x 7 | – Проактивный мониторинг ИБ<br>– Рекомендации, помощь в реагировании;<br>– Ежемесячные отчеты<br>– **Техническая поддержка оборудования ИБ** | 30 минут | 1-2 уровень |
| **AMTSOC-OUTSTF-STD** | 8 x 5 x onsite | – Проактивный мониторинг ИБ<br>– Рекомендации, помощь в реагировании;<br>– Ежемесячные отчеты<br>– **Эксплуатация на объекте** | – Online<br>– NBD | 1-2 уровень |
| **AMTSOC-OUTSTF-ADV** | 24 x 7 x onsite | – Проактивный мониторинг ИБ<br>– Рекомендации, помощь в реагировании;<br>– Ежемесячные отчеты<br>– **Эксплуатация на объекте** | Online | 1-2 уровень |

AMT GROUP

# Задачи аналитики в обеспечении ИБ





Оперативный уровень (специалисты ИБ/ ИТ)

Тактический уровень (CISO, руководство службы ИБ)

Стратегический уровень (TOP – менеджеры, кураторы ИБ)

AMT GROUP

# Оперативный уровень. Проблематика

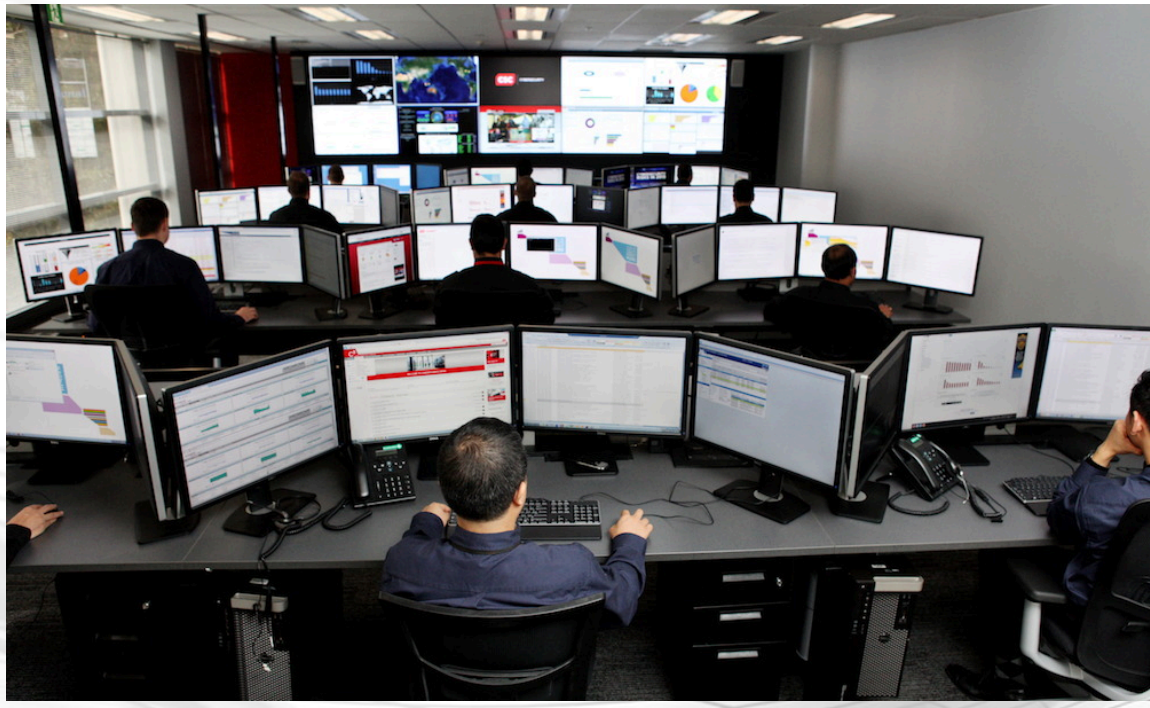


## Ограниченность средств визуализации и отчетности SIEM

- Штатных средств визуализации SIEM и других СЗИ недостаточно

## Необходимы дополнительные уровни корреляции

- Для интеграции с системами HR, СКУД, IT..



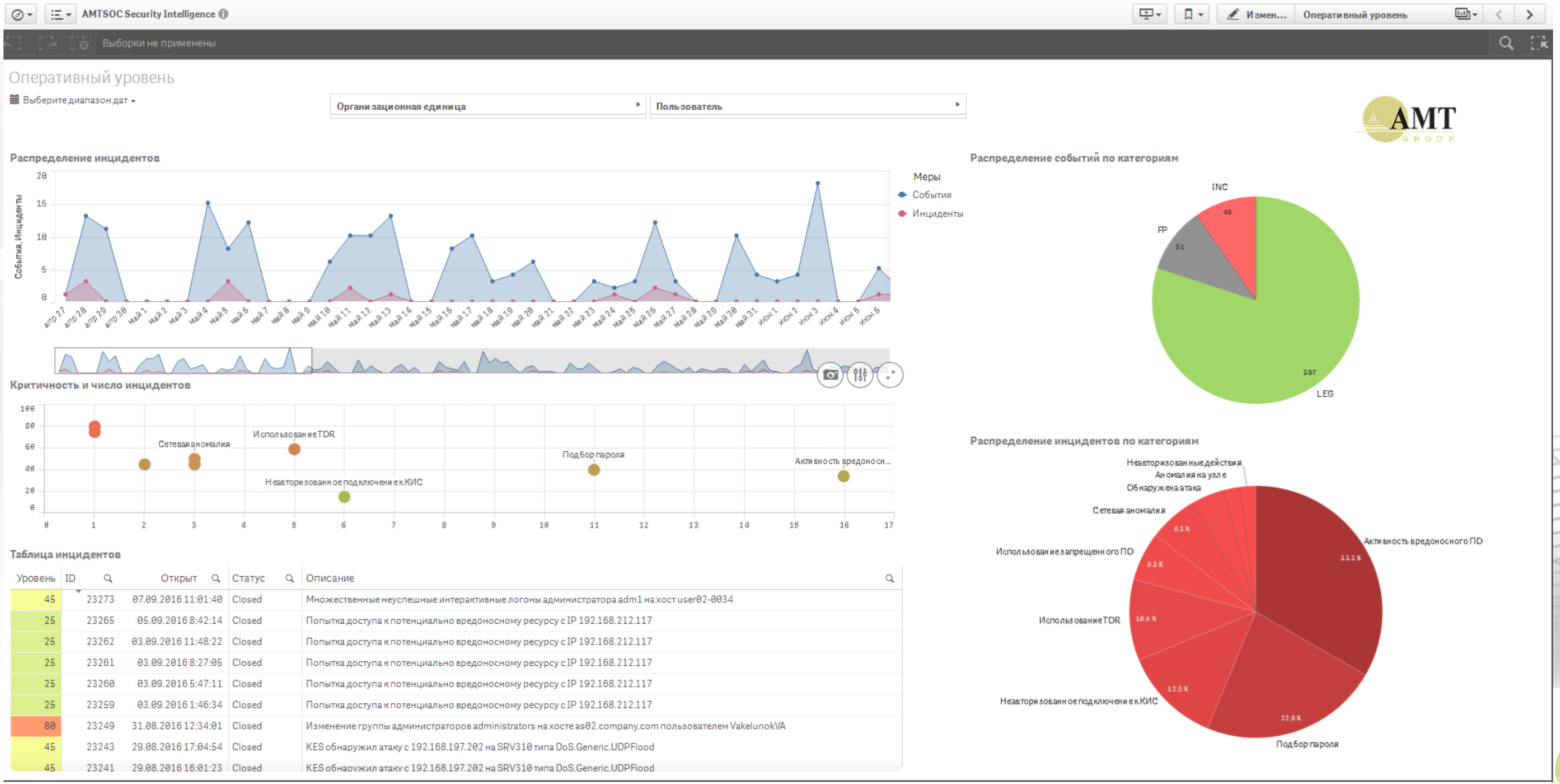
# Оперативный уровень. Примеры комплексных метрик




| | |
|---|---|
| Списки критичных инцидентов | СЗИ |
| Списки найденных уязвимостей | СЗИ |
| Распределение инцидентов по времени | СЗИ |
| Статистика по категориям инцидентов | СЗИ |
| Обнаруженные аномалии | СЗИ |

# Пример визуализации BI: Оперативный уровень






| Уровень | ID | Открыт | Статус | Описание |
|---|---|---|---|---|
| 45 | 23273 | 07.09.2016 11:01:40 | Closed | Множественные неуспешные интерактивные логоны администратора adm1 на хост user02-0034 |
| 25 | 23265 | 05.09.2016 8:42:14 | Closed | Попытка доступа к потенциально вредоносному ресурсу с IP 192.168.212.117 |
| 25 | 23262 | 03.09.2016 11:48:22 | Closed | Попытка доступа к потенциально вредоносному ресурсу с IP 192.168.212.117 |
| 25 | 23261 | 03.09.2016 8:27:05 | Closed | Попытка доступа к потенциально вредоносному ресурсу с IP 192.168.212.117 |
| 25 | 23260 | 03.09.2016 5:47:11 | Closed | Попытка доступа к потенциально вредоносному ресурсу с IP 192.168.212.117 |
| 25 | 23259 | 03.09.2016 1:46:34 | Closed | Попытка доступа к потенциально вредоносному ресурсу с IP 192.168.212.117 |
| 80 | 23249 | 31.08.2016 12:34:01 | Closed | Изменение группы администраторов administrators на хосте as02.company.com пользователем VakelunokVA |
| 45 | 23243 | 29.08.2016 17:04:54 | Closed | KES обнаружил атаку с 192.168.197.202 на SRV310 типа DoS.Generic.UDPFlood |
| 45 | 23241 | 29.08.2016 16:01:23 | Closed | KES обнаружил атаку с 192.168.197.202 на SRV310 типа DoS.Generic.UDPFlood |

AMT GROUP

# Тактический уровень. Проблематика



## Отслеживать метрики результативности процессов СУИБ (например, ISO/IEC 27001)

- Не все данные для расчета можно собрать из СЗИ

## Контролировать ИБ в нескольких удаленных офисах

- Не все СЗИ внедрены в удаленных офисах
- Не все из внедренных СЗИ позволяют построить «картинку» в нужном виде

## Оперативно отчитываться о состоянии ИБ руководству

- Оперативно сформировать отчет текущими средствами невозможно
- Комплексность видения/ «картинки» обратнопропорциональна оперативности

## Самому видеть комплексную картинку «на одном экране»

- Нет инструмента для построения «картинки» в нужном виде

# Тактический уровень. Примеры комплексных метрик




| | |
|---|---|
| Случаи изменения прав в обход установленного регламента, в т.ч. привилегированных пользователей | Портал самообслуживания (SD), IdM, отдельные ИС |
| Скорость устранения критичных уязвимостей (признанных актуальными для ИС) | СЗИ, корпоративный портал |
| Доля узлов, соответствующих политике ИБ (наличие АВЗ, средств мониторинга) | СЗИ |
| Своевременность и полнота выполнения резервного копирования информационных ресурсов | Система резервного копирования |
| Доля работников, прошедших обучение по ИБ, сведения об успешности сдачи тестов | HR, корпоративный портал |

AMT GROUP

# Тактический уровень «+++» . Примеры комплексных метрик

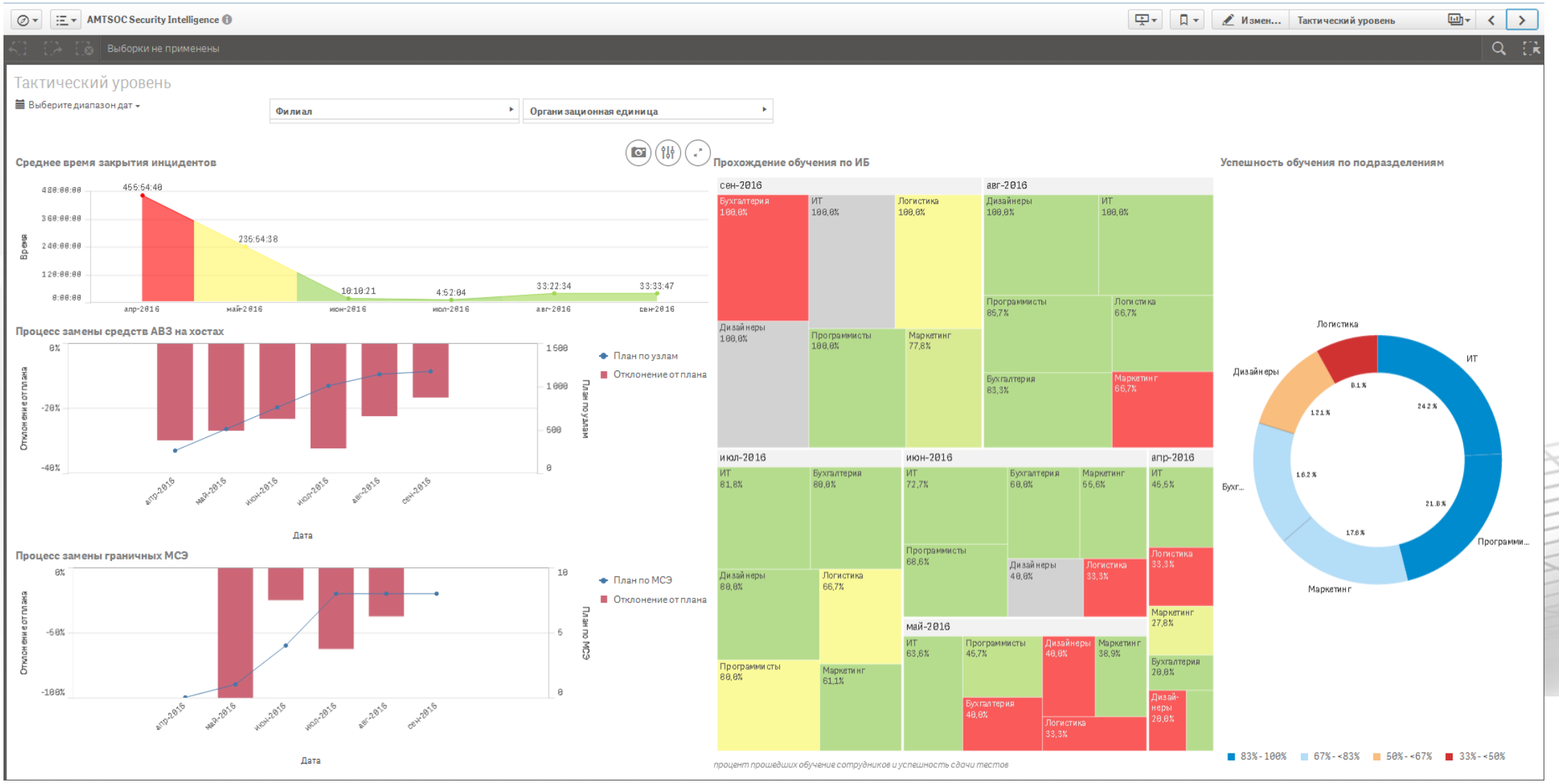



| | |
|---|---|
| Интегральный уровень риска организации | СЗИ, SD, корпоративный портал и др. |
| Соблюдение сроков реализации проектов ИБ | Корпоративный портал, xls-отчетность |
| Соответствие требованиям законодательства | Корпоративный портал, xls-отчетность |
| Длительность согласования ТЗ на доработку ИС со стороны службы ИБ | Корпоративный портал, SD |
| Время исполнения заявки на изменение прав доступа | Портал самообслуживания (SD), IdM, HR |
| Процент выполнение плана обработки рисков ИБ | Корпоративный портал, xls-отчетность |
| Актуальность документации СУИБ | Корпоративный портал (wiki), xls-отчетность |
| Результаты внутренней оценки зрелости процессов | Корпоративный портал (wiki), xls-отчетность |

AMT GROUP

# Пример визуализации BI: Тактический уровень





# Стратегический уровень. Проблематика



**Неинформативность для руководства низкоуровневых ИБ отчетов**

- Визуализация и отчеты ИБ для оперативного и тактического уровня не представляют интереса

**Отсутствие понимания эффективности работы службы ИБ**

- Метрики на оперативном и тактическом уровнях не показательны на топ-уровне;

**Нет понимания текущего уровня риска для основных бизнес-процессов и организации в целом**

- Нет возможности определить уровень риска (например в денежном исчислении)
- Нет корреляции процессов и событий/инцидентов ИБ с бизнес-процессами

**Нет единой комплексной картинки «на одном экране»**

- Нет инструмента для построения «картинки» в нужном виде

# Стратегический уровень. Примеры комплексных метрик

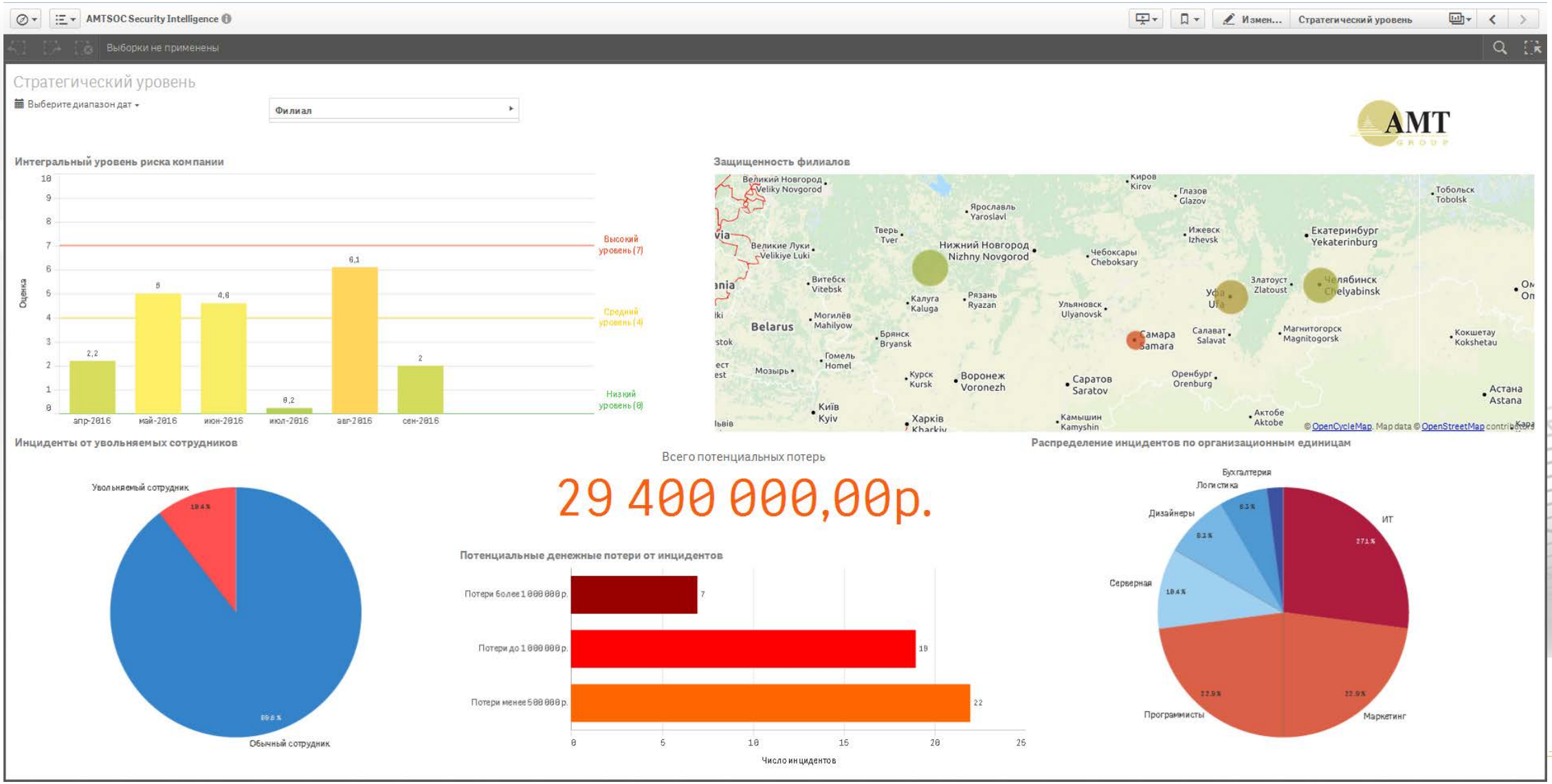



| | |
|---|---|
| Интегральный уровень риска компании | СЗИ |
| Геокарта с уровнем риска | СЗИ, IT |
| Доля участия в инцидентах различных подразделений, типов сотрудников | СЗИ, HR |
| Финансовые выражения потенциальных потерь от инцидентов ИБ | СЗИ, IT, экономический департамент |
| Влияние инцидентов ИБ на основные бизнес-процессы | СЗИ, IT, PM |

AMT GROUP

# Пример визуализации BI: Стратегический уровень






AMT GROUP

# Спасибо за внимание



## Вопросы?