МЕТОДИКИ КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ ДЛЯ ОБНАРУЖЕНИЯ ЦЕЛЕВЫХ АТАК

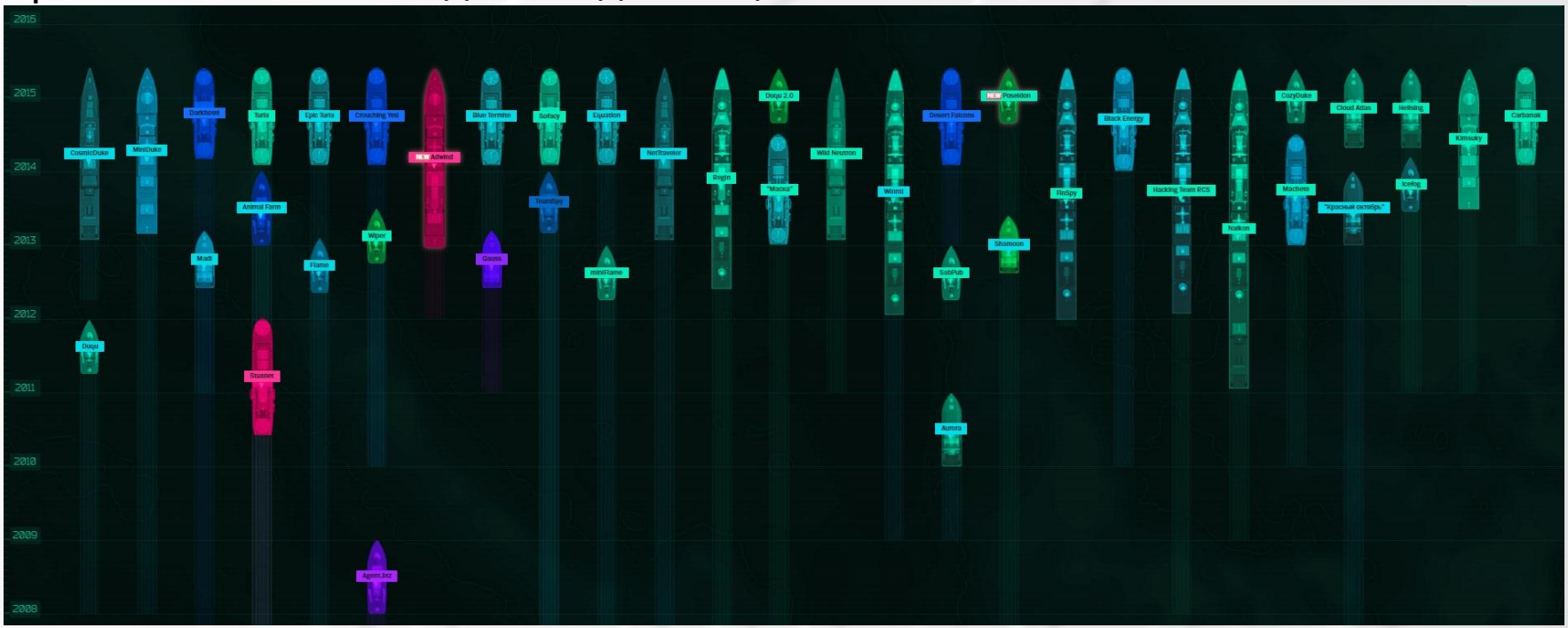
А.В. Федорченко, И.В. Котенко

СПИИРАН,
Санкт-Петербург, Россия

РусКрипто’2016, 22-25 марта 2016 г.

Целевые атаки (1/3)

Целевые атаки (Advanced Persistent Threat, APT) – класс компьютерных атак, направленных на достижение конкретных злонамеренных целей по отношению к выбранной жертве (компании, организации, службе, отрасли), использующих специально разработанные средства воздействия, а также ранее не известные механизмы проникновения и обхода методов защиты.



[Электронный ресурс: https://apt.securelist.com/ru/#secondPage]

Целевые атаки (2/3)

Свойства целевых атак и их зависимость

Целевые атаки (3/3)

Сравнение целевых и типовых атак

Свойство	Целевая атака	Типовая атака
Разнообразие методов атаки	Высокое (применяются всевозможные способы)	Низкое
Многоступенчатость атаки	Высокая	Низкая
Длительность атаки	Не ограниченная до достижения цели, либо до обнаружения факта атаки	Ограничена получением максимальной выгоды до обнаружения
Интенсивность атаки (этапа)	Низкая и (или) нестандартная	Максимально высокая, типичная для атаки (этапа)
Обманные атакующие действия	Высоковероятны и продуктивны	Маловероятны и малоэффективны
Действия для обхода конкретных средств защиты	Узконаправленные, рассчитанные на конкретные средства защиты атакуемой инфраструктуры	Если есть, то широконаправленные, рассчитанные на различные средства защиты и продукты
Точка входа	Любая, но стремиться к минимуму (одной точке), локализованная и избирательная в зависимости от вероятности обнаружения проникновения	Специфичная (в зависимости от конкретной атаки), но может быть распределенной (много точек) и глобальной (стремящейся к максимальному значению)
Физическая цель атаки	Максимально конкретная, локально сосредоточенная	Рассеянная, рассредоточенная
Логическая цель атаки	Рассчитана на конкретную выгоду от получения информации (доступ, хищение), либо нанесения преднамеренного ущерба (модификация, удаление)	Рассчитана на случайную выгоду при массовости распространения атаки

Обнаружение целевых атак (1/4)

Свойства атакующих действий, препятствующих обнаружению целевых кибератак обычными средствами:

- Использование средств социальной инженерии
- Эксплуатация 0-day уязвимостей
  - Распространенное АПО
  - Специальное (внутреннее) АПО
- Ограничение воздействия
- Воздействие на механизмы защиты

Непредсказуемость и неоднозначность действий при целевой атаке затрудняет их обнаружение существующими средствами защиты

Обнаружение целевых атак (2/4)

Проблемы обнаружения целевых атак

- Большой объем обрабатываемых данных
  - увеличение объема трафика
  - увеличение количества типов событий
- Отсутствие учета организационной структуры атакуемого объекта
- Сложность выявления внутреннего нарушителя
- Большое количество ложных срабатываний

Задачи обнаружения целевых атак

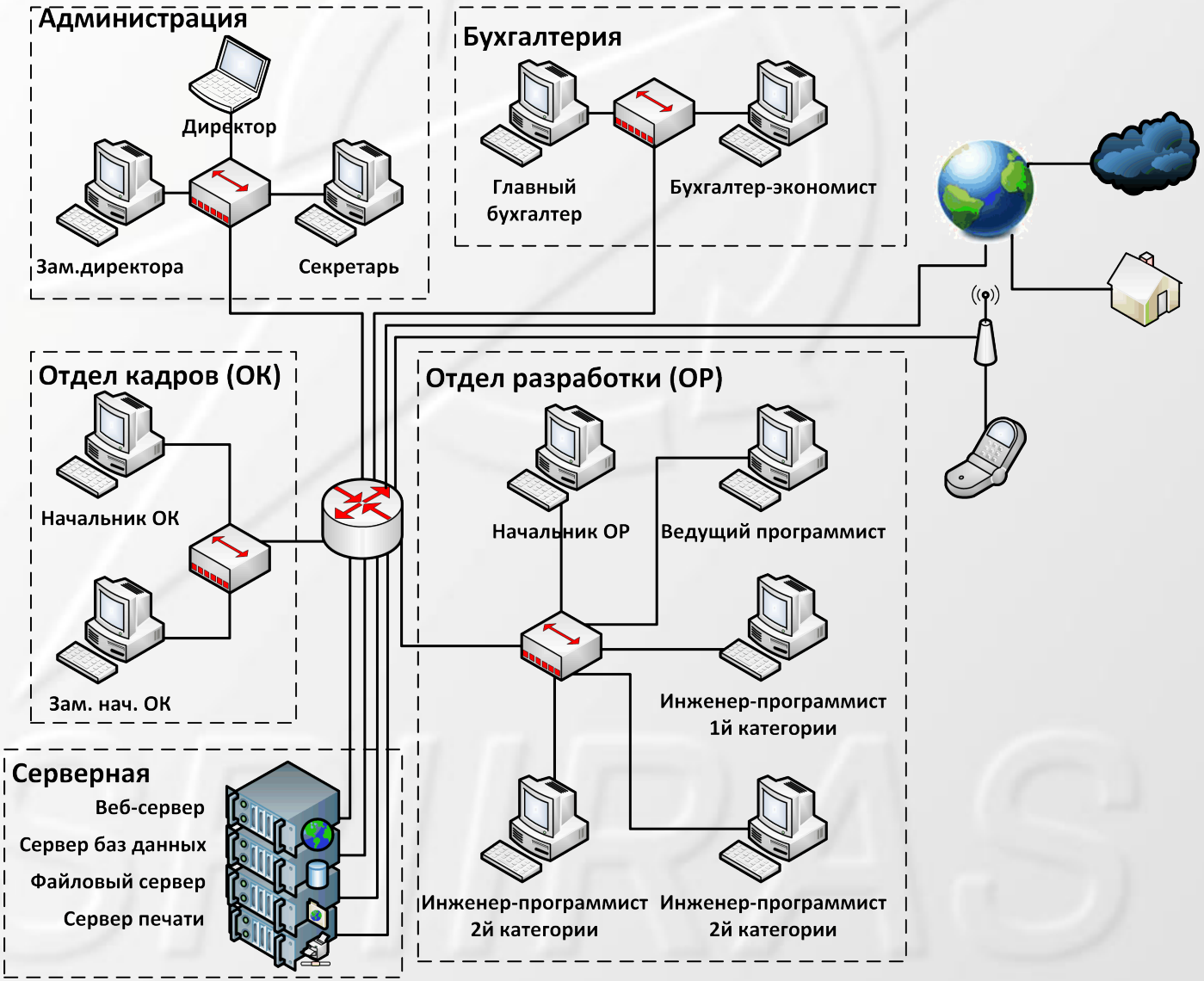
1. **Детектирование атакующего действия**
2. Поиск предшествующих атакующих действий в рамках целевой атаки
3. Прогнозирование последующих атакующих действий в рамках целевой атаки
4. Определение цели атаки

Обнаружение целевых атак (3/4)

Общая концепция корреляции событий
для обнаружения целевых атак

- Обеспечение связи событий физического периметра и информационного пространства, с учетом структурных подразделений (департамент, отдел, группа и др.) защищаемого объекта
- Учет важности внутренних активов
- Учет политики безопасности в отношении сотрудников
- Контроль действий сотрудников в рамках удаленного взаимодействия с внутренней инфраструктурой

Обнаружение целевых атак (4/4)



Корреляция событий (1/4)

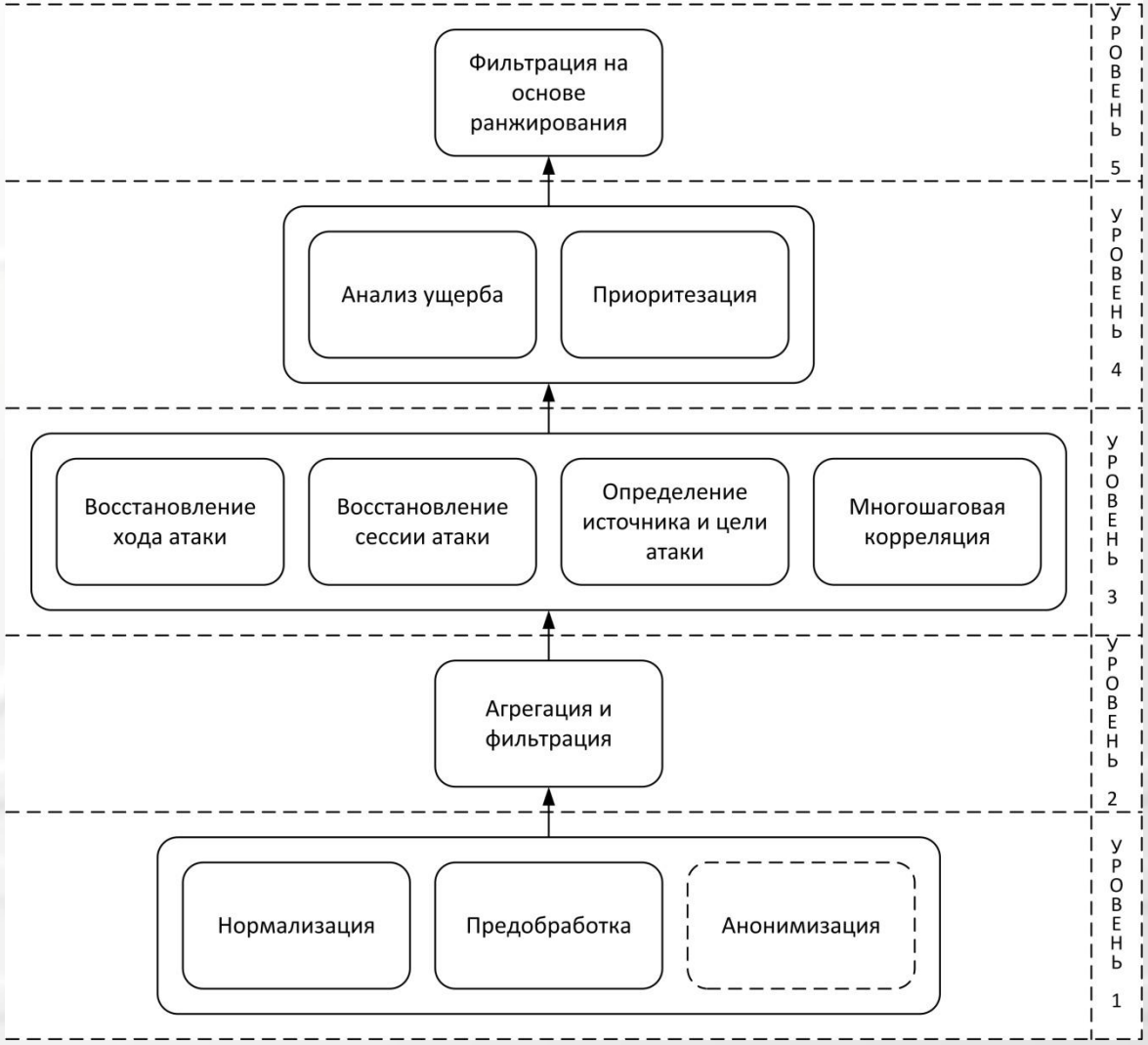
Метод корреляции включает последовательность действий над данными, направленную на выявление и (или) применение определенным способом признаков удаления, объединения, связывания, установления причинности и приоритетности обрабатываемых событий.

Классификация методов корреляции

- По возможности изменения корреляционных признаков
  - статические
  - динамические
- По способу изменения корреляционных признаков
  - самообучаемые
  - изменяемые вручную
  - неизменяемые
- По типу вычисления результата
  - упорядоченные
  - вероятностные
  - смешанные

Корреляция событий (2/4)

Обобщенная иерархическая схема процесса корреляции

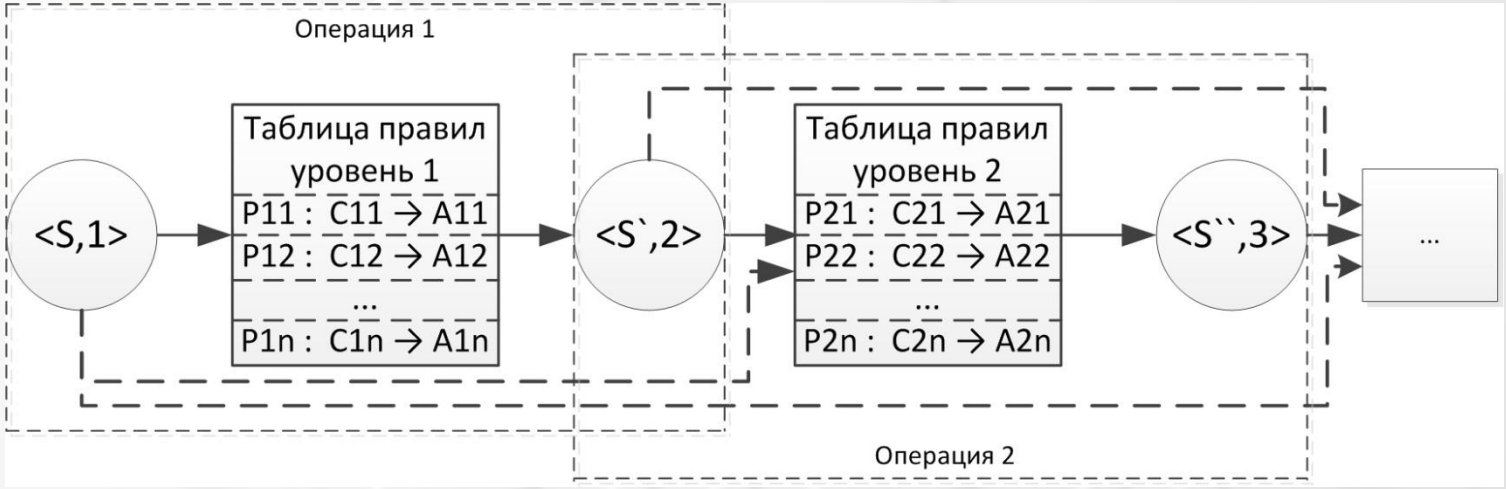


Корреляция событий (3/4)

Основные методы корреляции

- Правило-ориентированный (Rule based)
- Конечный автомат (Finite state machine)
- Вывод на основе прецедентов (Case based reasoning)
- Сеть Байеса (Bayesian network)
- Искусственные нейронные сети (Neural network)

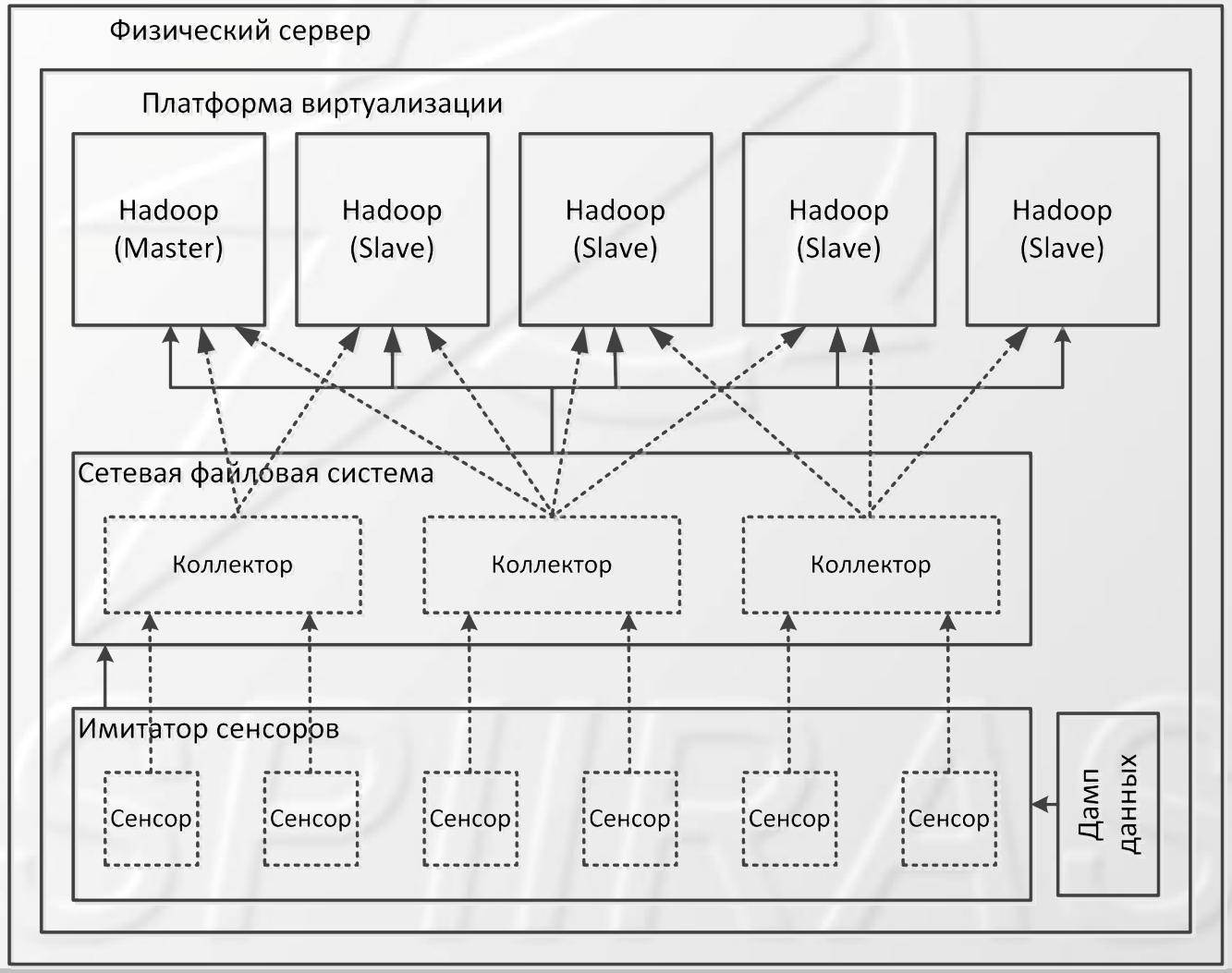
Реализация правило-ориентированного метода



S - поток событий, *P* - правило, *C* - условие выполнения правила, *A* - действие правила

Корреляция событий (4/4)

Распределенная архитектура стенда корреляции событий безопасности



Заключение

- Рассмотрены свойства и особенности целевых атак
- Выделены проблемы обнаружения целевых атак типичными средствами защиты
- Определена общая концепция корреляции событий безопасности для обнаружения целевых атак
- Представлена архитектура стенда корреляции, ориентированная на обработку больших данных

Контактная информация

Федорченко Андрей Владимирович
fedorchenko@comsec.spb.ru

Котенко Игорь Витальевич
http://comsec.spb.ru/en/staff/kotenko
ivkote@comsec.spb.ru

Благодарности

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН