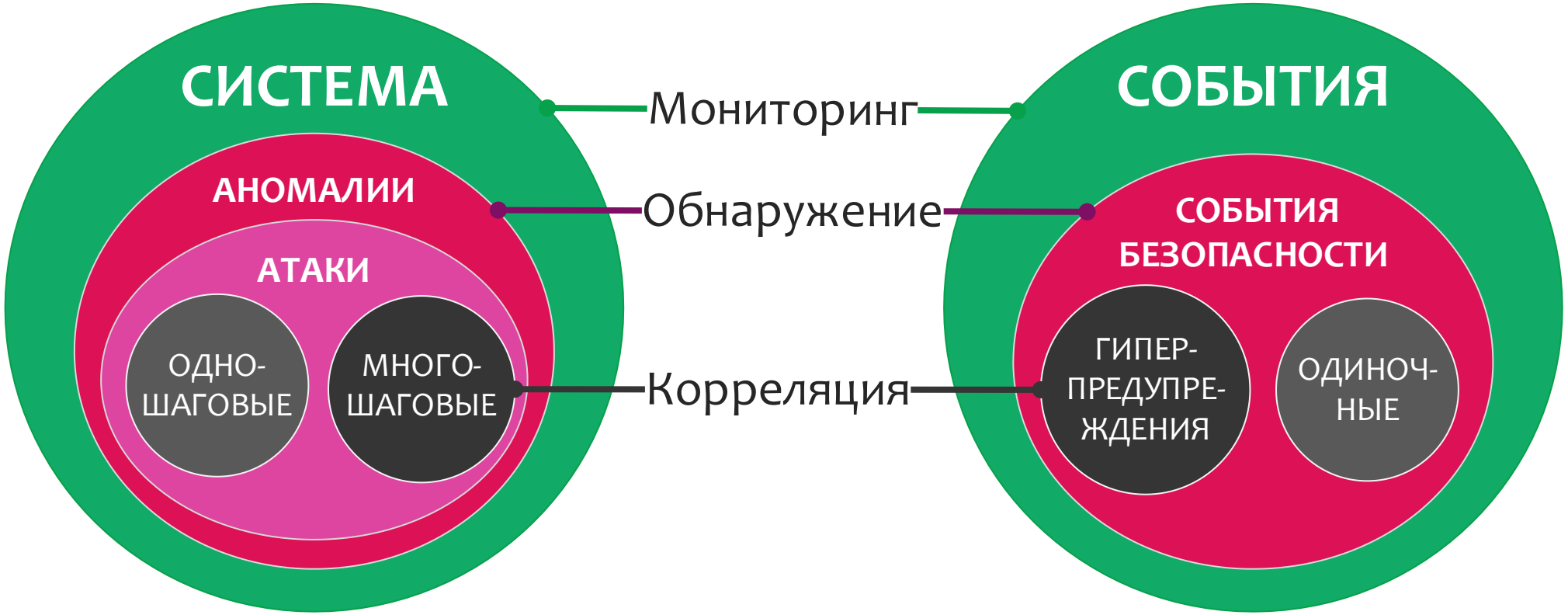
Ежегодная международная научно-практическая конференция «РусКрипто'2022»

Интеллектуальные методы корреляции событий кибербезопасности

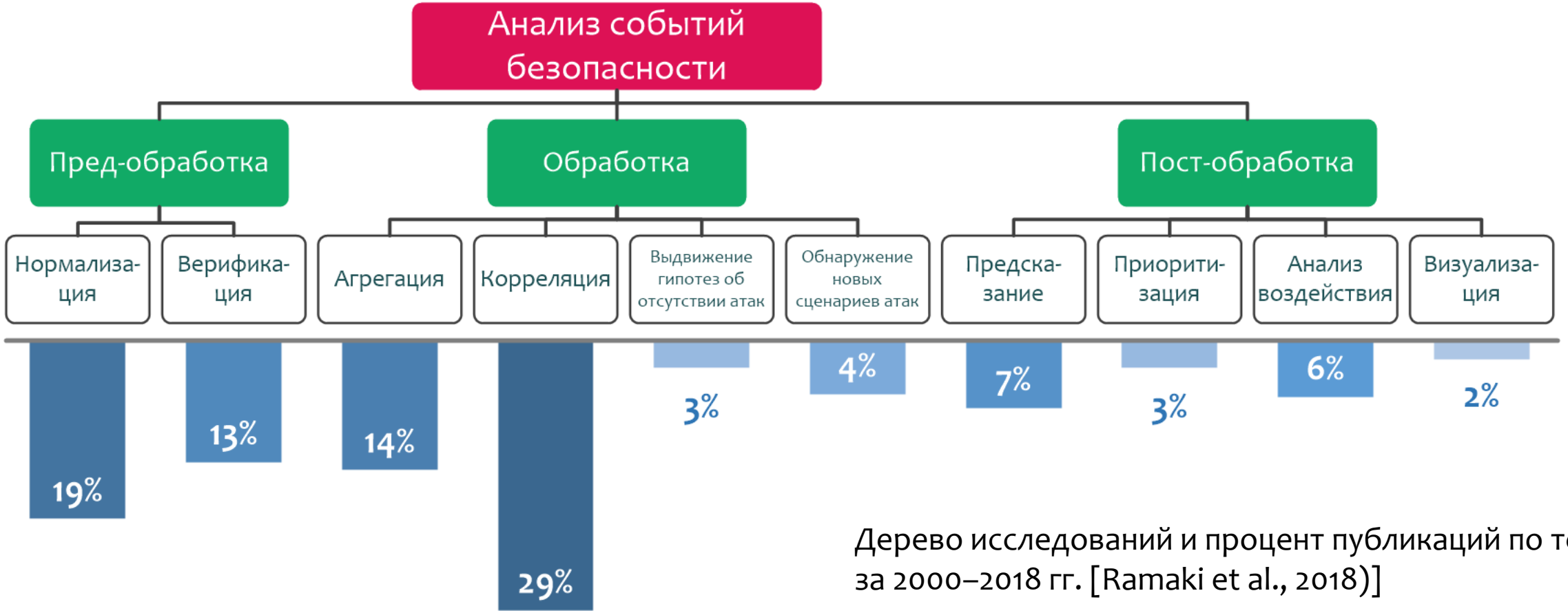
Котенко Игорь Витальевич, д.т.н., профессор, СПб ФИЦ РАН
Гайфулина Диана Альбертовна, аспирант, СПб ФИЦ РАН

Содержание

Управление событиями безопасности и обнаружение атак



Темы исследований в области анализа событий безопасности



Дерево исследований и процент публикаций по теме за 2000–2018 гг. [Ramaki et al., 2018)]

Подход к классификации методов корреляции в релевантных исследованиях

Методы корреляции на основе сходства – Модель обнаружения аномалий на основе корреляции (1/2)

Источник: **Hostiadi et al. (2019)**

Поток трафика (*FT*) – это набор предупреждений, состоящий из:

$$FT=\{ft_1, ft_2, \ldots, ft_j\},\ ft = \{(srcIP, dstIP, sport, dport, pcl, lgh, cnt)\},$$

где *srcIP* – IP-адрес источника, *dstIP* – IP-адрес назначения, *sport* – адрес порта источника, *dport* – адрес порта назначения, *pcl* – протокол, *lgh* – длина, *cnt* – количество.

Сходство IP-адреса – это полное сходство между $(srcIP_{fti}, srcIP_{ftj})$ и $(dstIP_{fti}, dstIP_{ftj})$, где сходство IP-адреса рассчитывается по формуле:

$$sim(IP_i, IP_j) = bm/\sigma,$$

где *bm* – количество совпадений битов двух сравниваемых IP-адресов, а σ – общая длина IP-адреса в битах.

Сходство адреса порта – это полное сходство между $(sport_{fti}, sport_{ftj})$ и $(dport_{fti}, dport_{ftj})$:

$$sim(port_{fti}, port_{ftj}) = 1, \text{ если } port_{fti}=port_{ftj}, \text{ или 0, если } port_{fti}\neq port_{ftj}.$$

Сходство длины – это сходство между (lgh_{fti}, lgh_{ftj}):

$$sim(lgh_{fti}, lgh_{ftj}) = 1, \text{ если } lgh_{fti}=lgh_{ftj}, \text{ или 0, если } lgh_{fti}\neq lgh_{ftj}.$$

Сходство количества – это сходство между значениями (cnt_{fti}, cnt_{ftj}):

$$sim(cnt_{fti}, cnt_{ftj}) = 1, \text{ если } cnt_{fti}=cnt_{ftj}, \text{ или 0, если } cnt_{fti}\neq cnt_{ftj}.$$

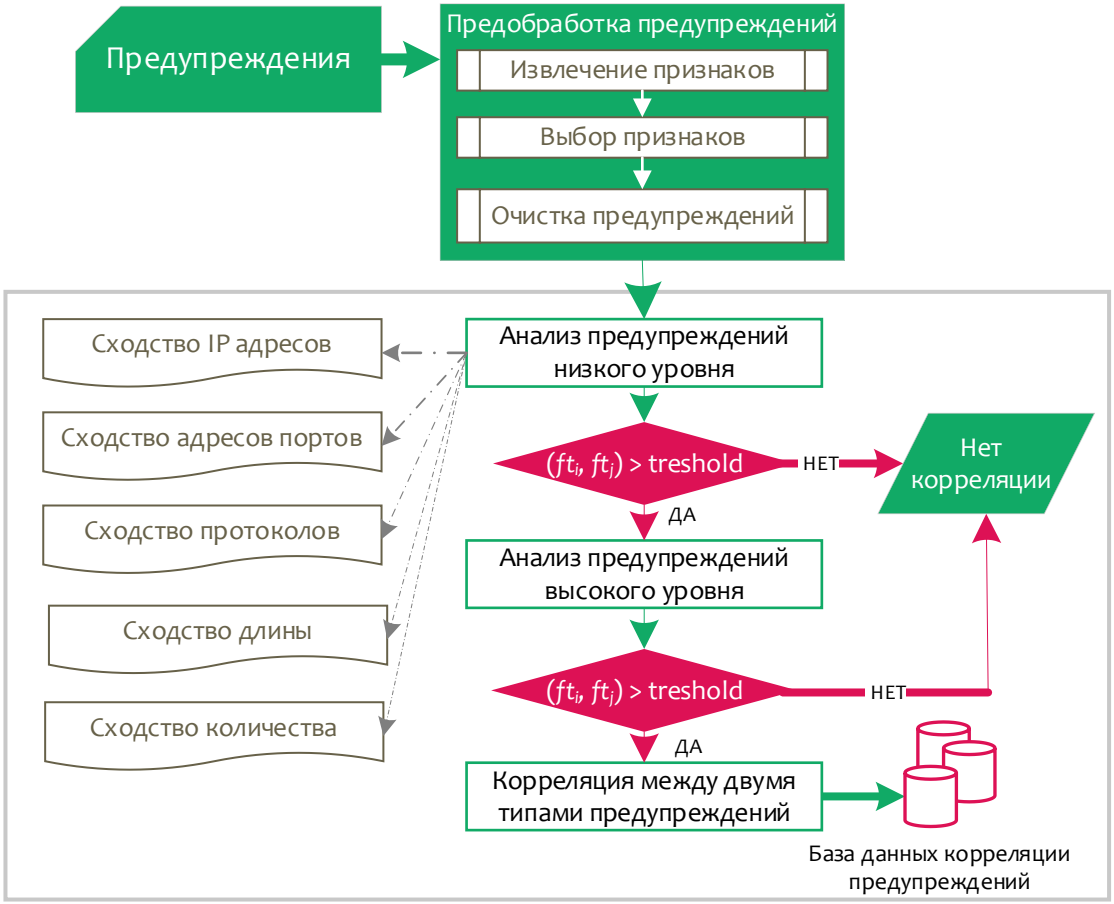
Методы корреляции на основе сходства – Модель обнаружения аномалий на основе корреляции (2/2)

Анализ предупреждений низкого уровня, обозначаемый как (Φ), представляет собой измерение сходства между потоками трафика (ft_i, ft_j) по типам аналогичных предупреждений на основе сходства между сравниваемыми атрибутами:

$$\Phi_i(ft_i, ft_j) = \{(sim(IP_i, IP_j), sim(port_{fti}, port_{ftj}), sim(lgh_{fti}, lgh_{ftj}), sim(cnt_{fti}, cnt_{ftj}))\}.$$

Анализ предупреждений высокого уровня, обозначаемый как (ϖ), представляет собой измерение сходства между двумя разными типами предупреждений. Пусть (Φ_i) — первый тип оповещения, отличный от оповещения второго типа (Φ_j), тогда значение сходства (ϖ) получается путем вычисления сходства двух типов оповещений (Φ_i, Φ_j), путем измерения с использованием:

$$\varpi = sim(\Phi_i, \Phi_j), \text{ где } \Phi_i \neq \Phi_j$$



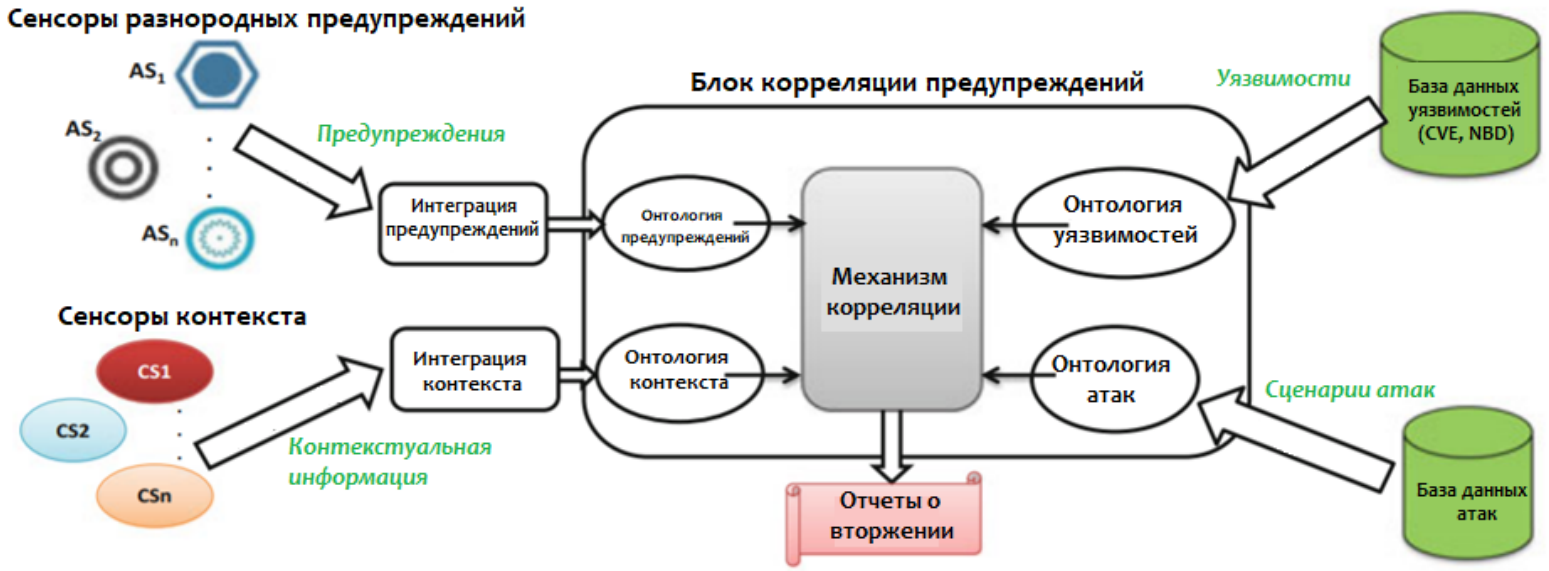
Предложенная модель **Hostiadi et al. (2019)**

Методы на основе сценариев:

Основанная на онтологии система корреляции предупреждений с учетом контекста

Источник: **Sadighian et al. (2013)**

1. Сбор предупреждений и контекста
2. Интеграция предупреждений и контекста
3. Заполнение онтологий
4. Корреляция предупреждений в онтологиях



- Онтология предупреждений: атрибуты предупреждений, такие как источник, цель, время и датчик.
- Онтология контекста: статическая контекстная информация (например, сетевая архитектура, профили хоста/пользователя и тип ОС) и динамическая контекстная информация (например, тип трафика, использование системы, время дня/недели).
- Онтология уязвимостей: уязвимости, связанные с существующими активами.
- Онтология атаки: известные сценарии атаки, включая общие атрибуты атаки, такие как векторы, цели и т. д.

Модель предпосылок и последствий:
Реконструкция сценариев атак с учетом семантики

Фреймворк реконструкции сценария атаки

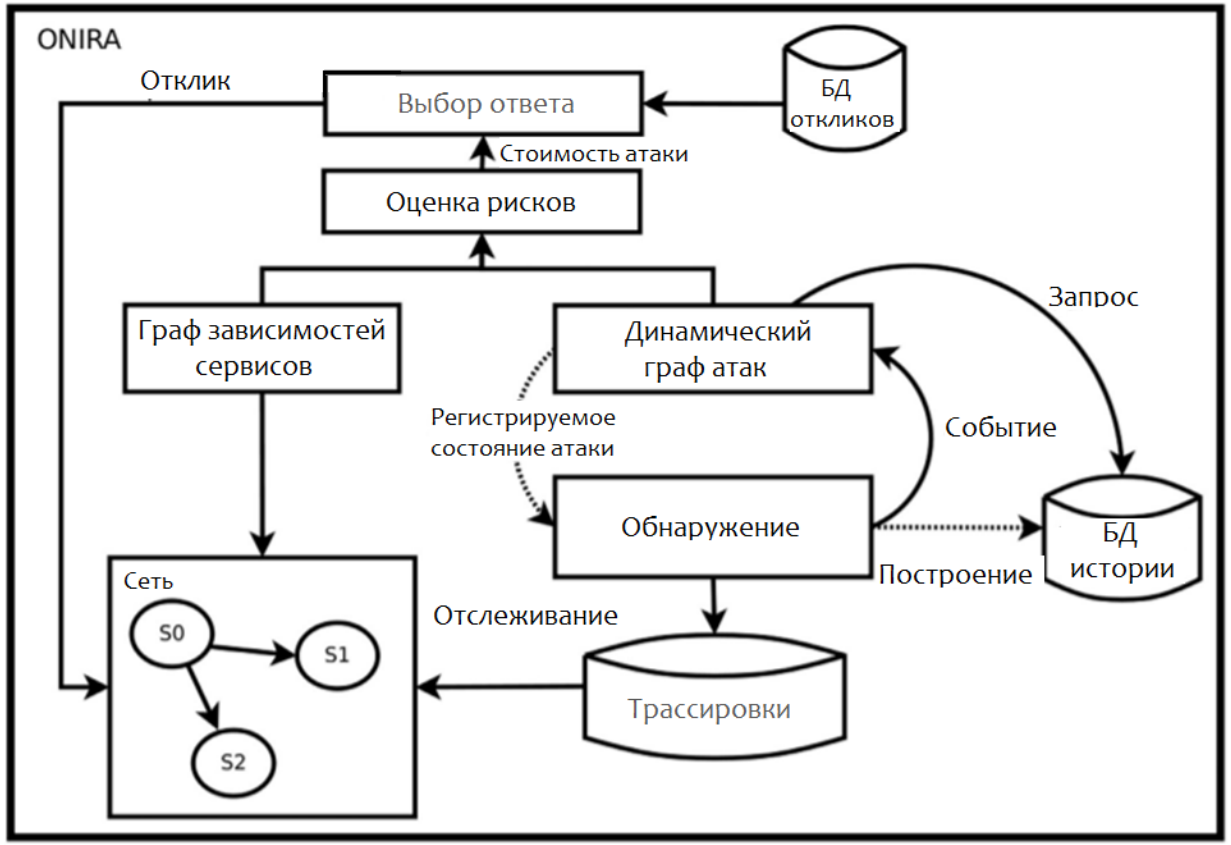
Источник: **Saad et al. (2013)**

Предлагаемый фреймворк извлечения сценария атаки состоит из следующих пяти компонентов:

1. база знаний,
2. нормализация предупреждений,
3. проверка предупреждений,
4. агрегация предупреждений,
5. корреляция предупреждений.

Графы и деревья атак:

Модель оценки риска вторжений на основе графов атак и зависимостей сервисов



Параметры графа атак

Параметры воздействия атаки =
{уровень знаний, влияние на КЦД[1],
частота атак,

прямое воздействие, обратное воздействие}

Параметры графа зависимостей сервисов

Онлайн-оценка риска вторжений распределенных трассировок с использованием архитектуры ONIRA (Online Intrusion Risk Assessment). *Источник*: **Shameli-Sendi et al. (2018)**

[1]КЦД – конфиденциальность, целостность, доступность

Графы и деревья атак:

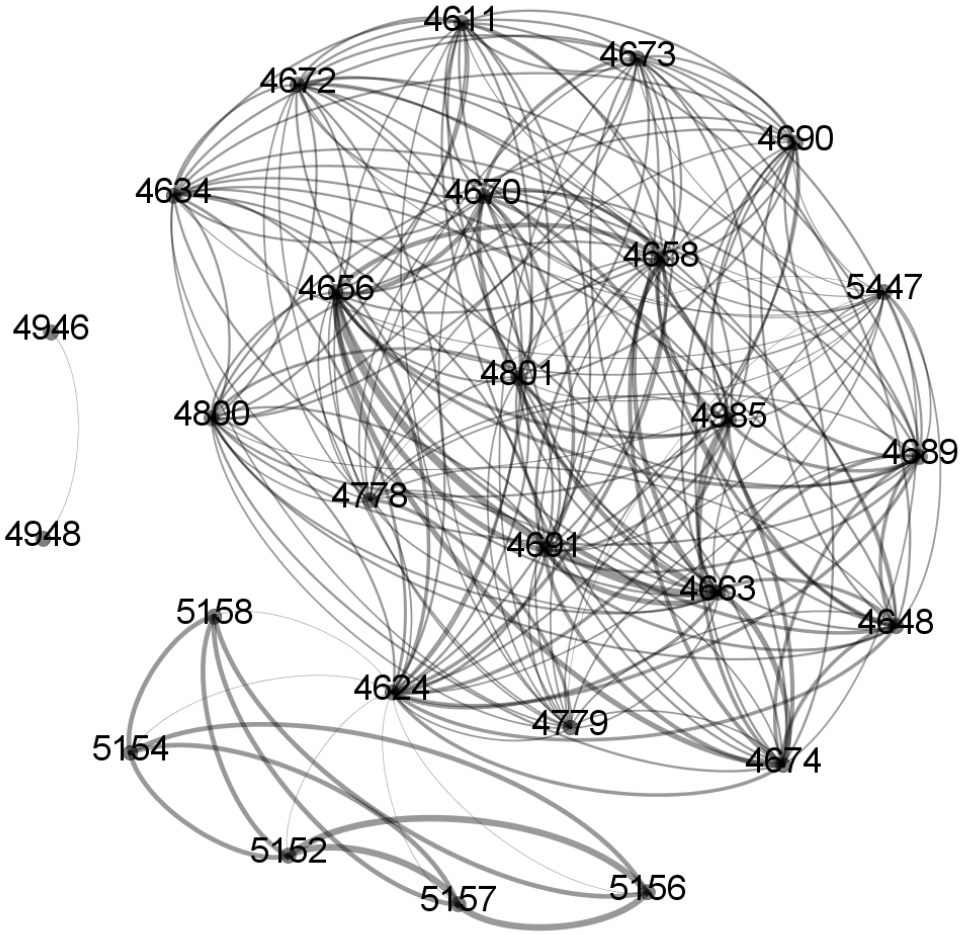
Структурный анализ событий безопасности

Источник: **Kotenko et al. (2018)**

Удельный вес (Wabs) связи между типами событий определяется количеством равнозначных свойств (при структурном анализе).

Относительный вес (Wrel) связи между событиями определяется количеством совпадающих значений равнозначных свойств в обрабатываемой паре событий.

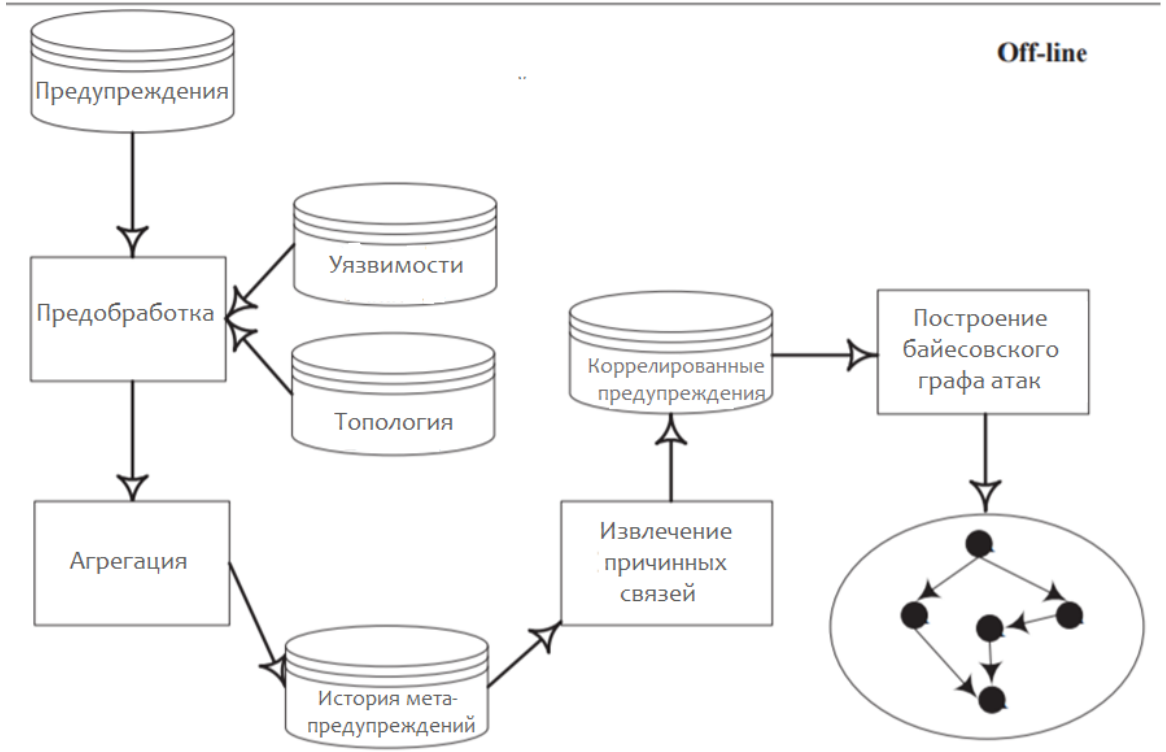
Результат выполнения корреляции над выборкой событий – получение набора пар значений: относительный вес, интервал времени (в пределах выбранного временного окна).



Статистические методы:

Корреляция предупреждений в реальном времени и прогнозирование с использованием байесовских сетей

Источник: **Ramaki et al. (2015)**



Предлагаемая корреляция предупреждений в автономном (офлайн) режиме

Предлагаемая корреляция предупреждений в онлайн режиме

Машинное обучение:

Прогнозирование событий безопасности на основе глубокого обучения

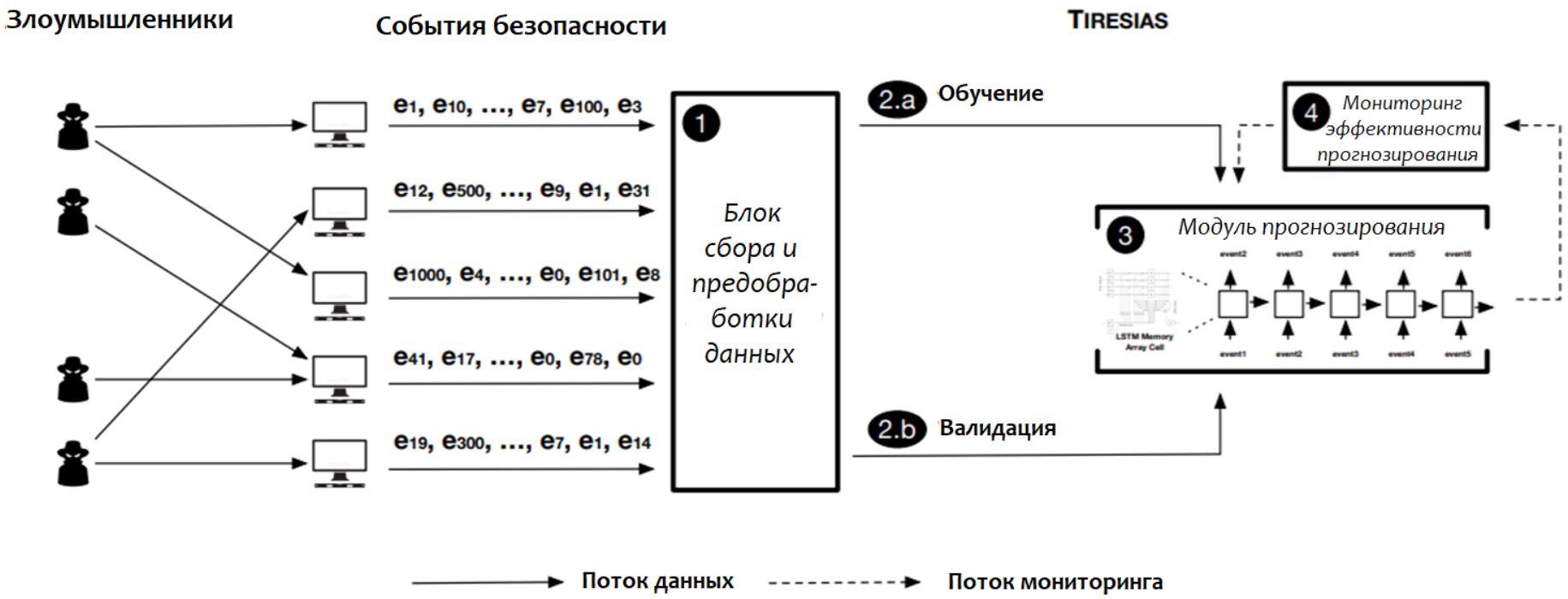
Источник: **Shen et al. (2018)**

S_1 $\ominus_{14}\ominus_{15}$ … $\mathbf{e_{10}}\ominus_{20}\mathbf{e_{11}e_8e_{12}e_4e_5}$ … $\mathbf{e_{12}e_{11}e_0e_3e_9}\ominus_{23}\mathbf{e_4e_9e_3e_4e_3e_9}\ominus_{23}\mathbf{e_3e_9}\ominus_{19}\ominus_{24}\ominus_{25}\ominus_{26}\mathbf{e_{12}e_{13}}$

S_2 $\mathbf{e_4}\ominus_{27}\mathbf{e_{10}e_{11}e_{12}}\ominus_{28}\mathbf{e_5}\ominus_{21}\mathbf{e_7}$ … $\mathbf{e_4}\ominus_{19}\ominus_{30}\ominus_{25}\ominus_{24}\ominus_{31}\mathbf{e_{12}}$

S_3 $\mathbf{e_4}\ominus_{41}$ … $\mathbf{e_5}\ominus_{22}\ominus_{21}\mathbf{e_7e_{12}}$ … $\mathbf{e_9e_3e_9e_3}$ … $\mathbf{e_6}\ominus_{23}\ominus_{19}\ominus_{30}\ominus_{25}\ominus_{24}\mathbf{e_{12}}$

Три конечные точки (S) подвергаются скоординированной атаке. {e0, ..., e13} — события, участвующие в скоординированной атаке, выделены жирным шрифтом.



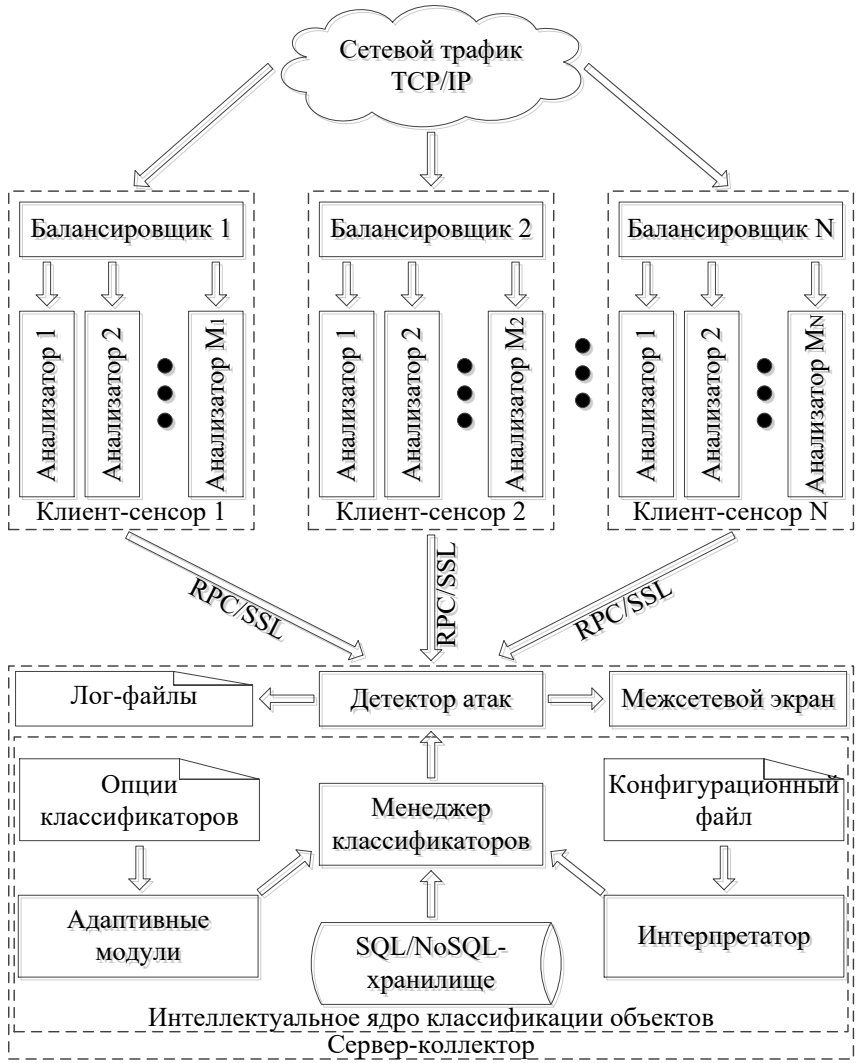
Последовательные события безопасности собираются, предварительно обрабатываются, а затем используются для построения и проверки прогностической модели. Затем оптимальная модель используется в операциях, и ее эффективность контролируется для обеспечения стабильно высокой точности прогноза.

Машинное обучение:

Система обнаружения сетевых событий

Источник: **Kotenko et al. (2018)**

- Ускоренная обработка сетевого трафика и сборки TCP/IP-сессий за счет механизма преаллокации динамической памяти, fnv-хеширования сетевых соединений, встроенных балансировщиков и алгоритма обхода многократно вложенных списков с параметрами сетевых соединений
- Алгоритм вычисления статистических параметров сетевого трафика на основе метода скользящей средней
- Набор сенсоров с поддержкой нескольких параллельных модификаций алгоритмов шаблонного поиска подстроки
- Безопасный канал передачи данных между клиентскими сенсорами и сервером на основе протокола RPC, зашифрованного при помощи SSL
- Хранение обучающих выборок в нескольких форматах баз данных (MySQL, MongoDB, *.csv)



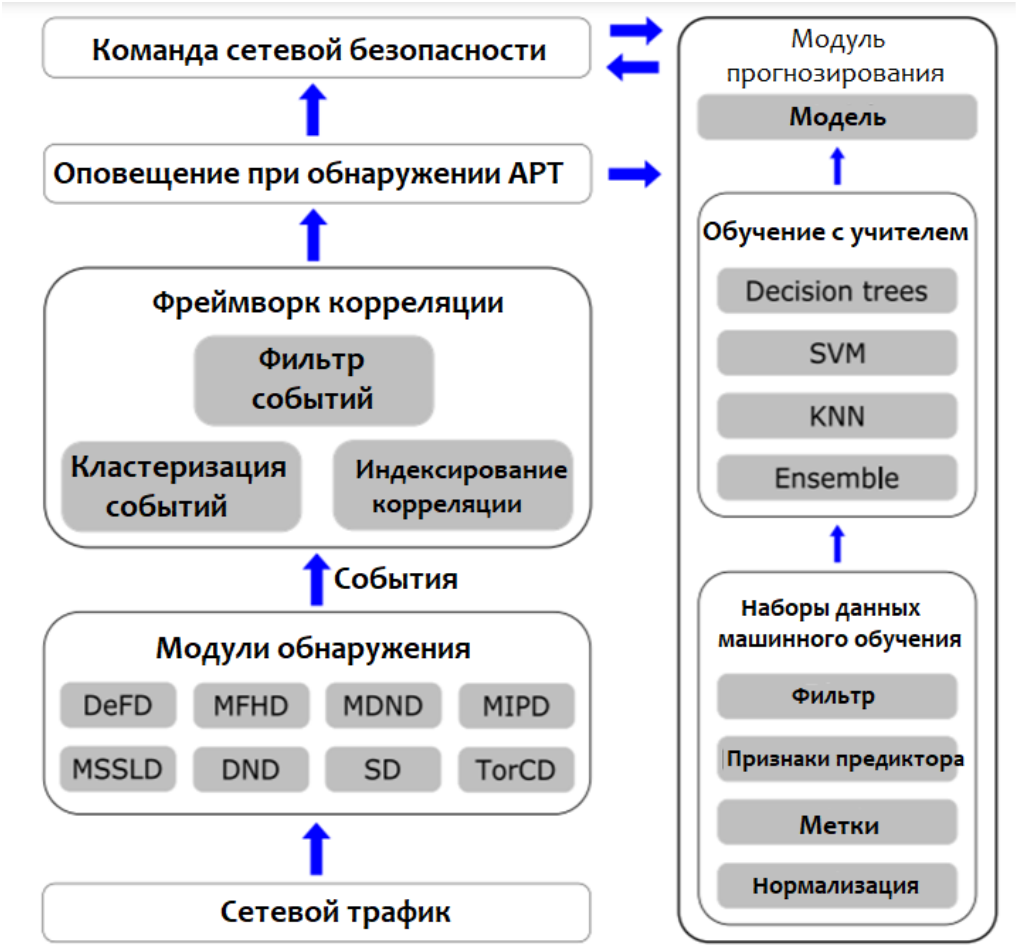
Смешанные методы корреляции:

Обнаружение APT с помощью корреляционного анализа и машинного обучения

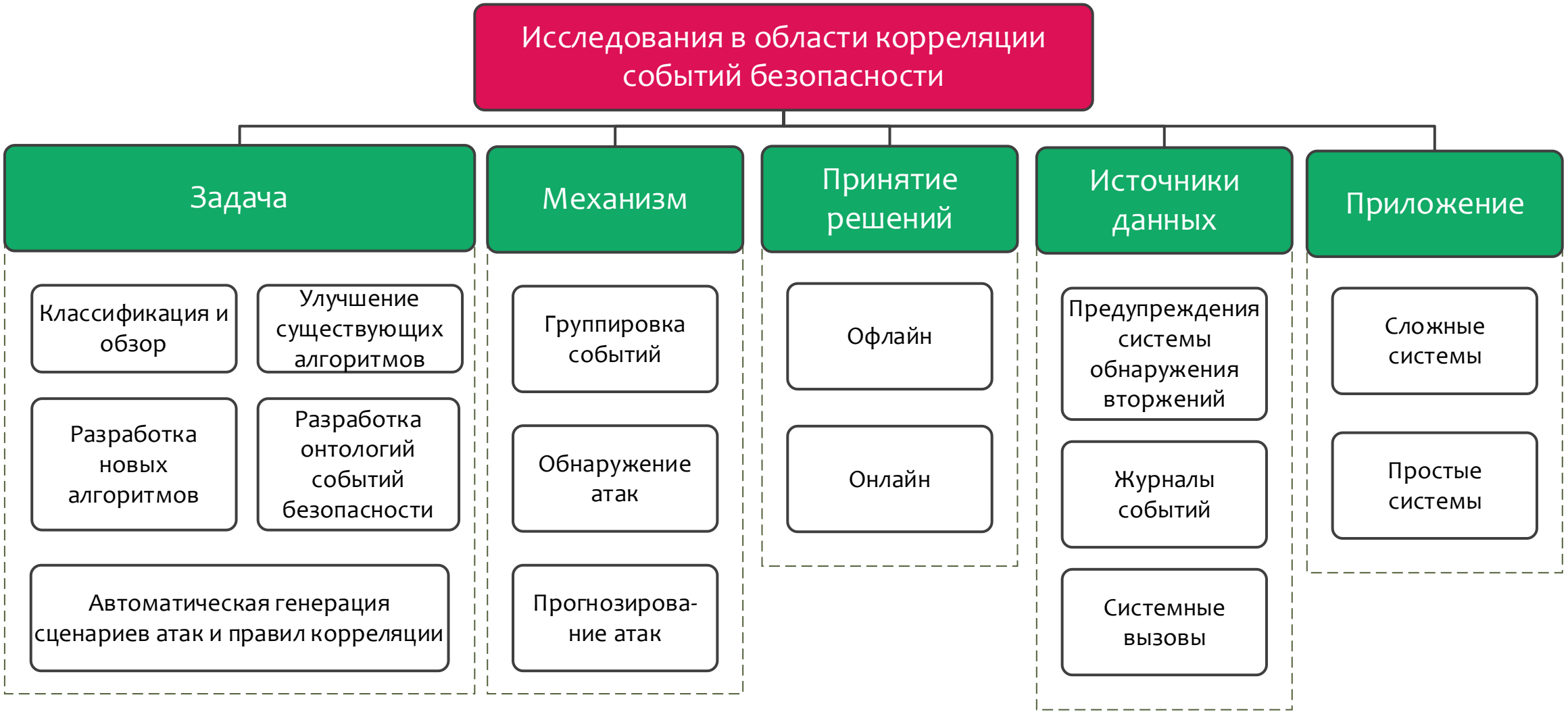
Источник: **Ghafir et al. (2018)**

Целью фреймворка корреляции является поиск событий безопасности, которые могут быть связаны и принадлежать одному сценарию атаки APT: *фильтр событий* для выявления избыточных или повторяющихся событий безопасности; *кластеризация событий*, которые, скорее всего, относятся к одному и тому же сценарию APT-атаки; и *индексирование корреляции* для оценки степени корреляции между событиями безопасности каждого кластера.

Модуль прогнозирования на основе машинного обучения используется командой сетевой безопасности для определения вероятности ранних событий безопасности для развития полной APT-атаки. Это позволяет *команде сетевой безопасности* прогнозировать атаку APT на ее ранних этапах и применять необходимые процедуры, чтобы остановить ее до завершения и свести к минимуму ущерб.



Основные направления исследований



Основные проблемы и будущие направления исследований

Проблема	Перспектива
Сокрытие вредоносных следов злоумышленником в многошаговой атаке	Использование методов анализа семантики событий безопасности
	Корреляция событий безопасности для прогнозной аналитики
Объяснимость семантики событий безопасности	Разработка онтологий и графов знаний о событиях
Анализ кардинальных событий безопасности	
Постоянная поддержка баз знаний о событиях и связях между ними	Разработка и использование самообучающихся баз знаний событий
Анализ гетерогенных и/или больших объемов данных о событиях безопасности	Поддержка распределенной корреляции событий и обработки больших данных
	Поддержка нормализации и унификации событий безопасности
Низкая доступность актуальных открытых датасетов	Разработка новых наборов данных и предоставление доступа для широкого круга исследователей

Спасибо за внимание!

Контактная информация

Электронная почта:

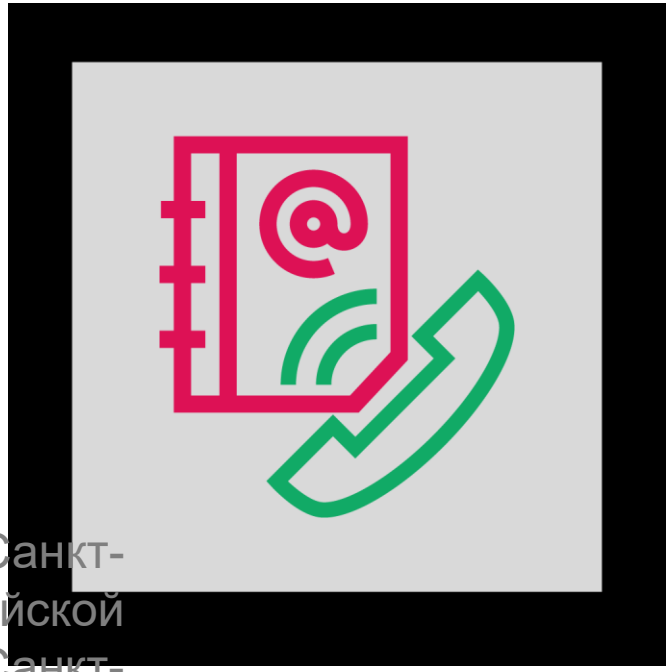
Котенко Игорь Витальевич:

ivkote@comsec.spb.ru

Гайфулина Диана Альбертовна:

gaifulina@comsec.spb.ru

Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН). 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, Россия



Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.