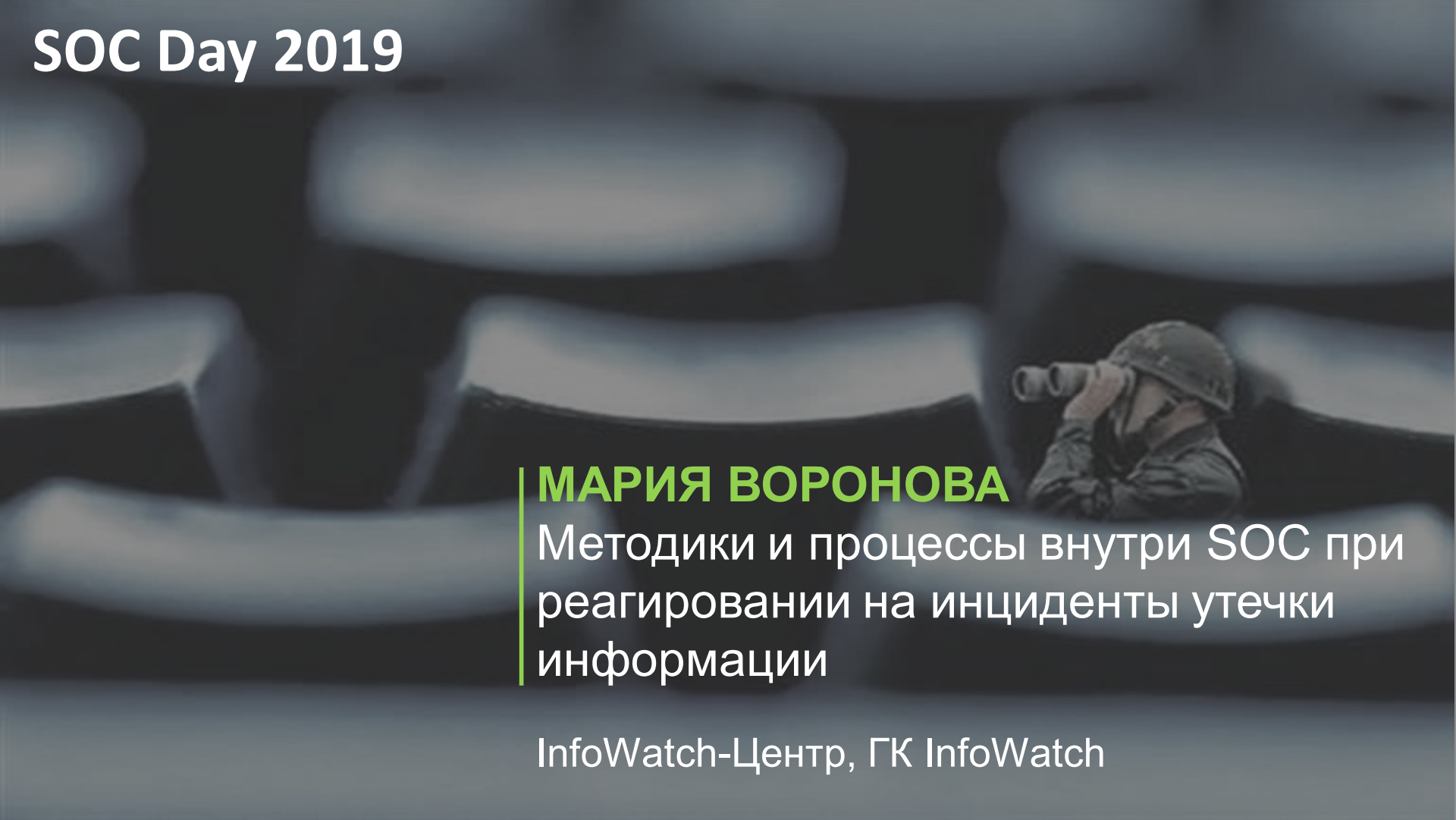
SOC Day 2019



МАРИЯ ВОРОНОВА

Методики и процессы внутри SOC при реагировании на инциденты утечки информации

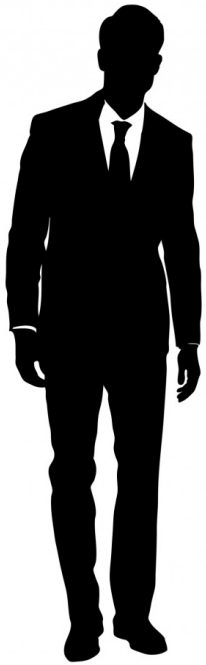
InfoWatch-Центр, ГК InfoWatch

Актуальное инсайдерство

INFOWATCH®

Утечка сведений, составляющих государственную, коммерческую тайну или иную информацию ограниченного доступа

Нелояльное поведение работников, саботаж



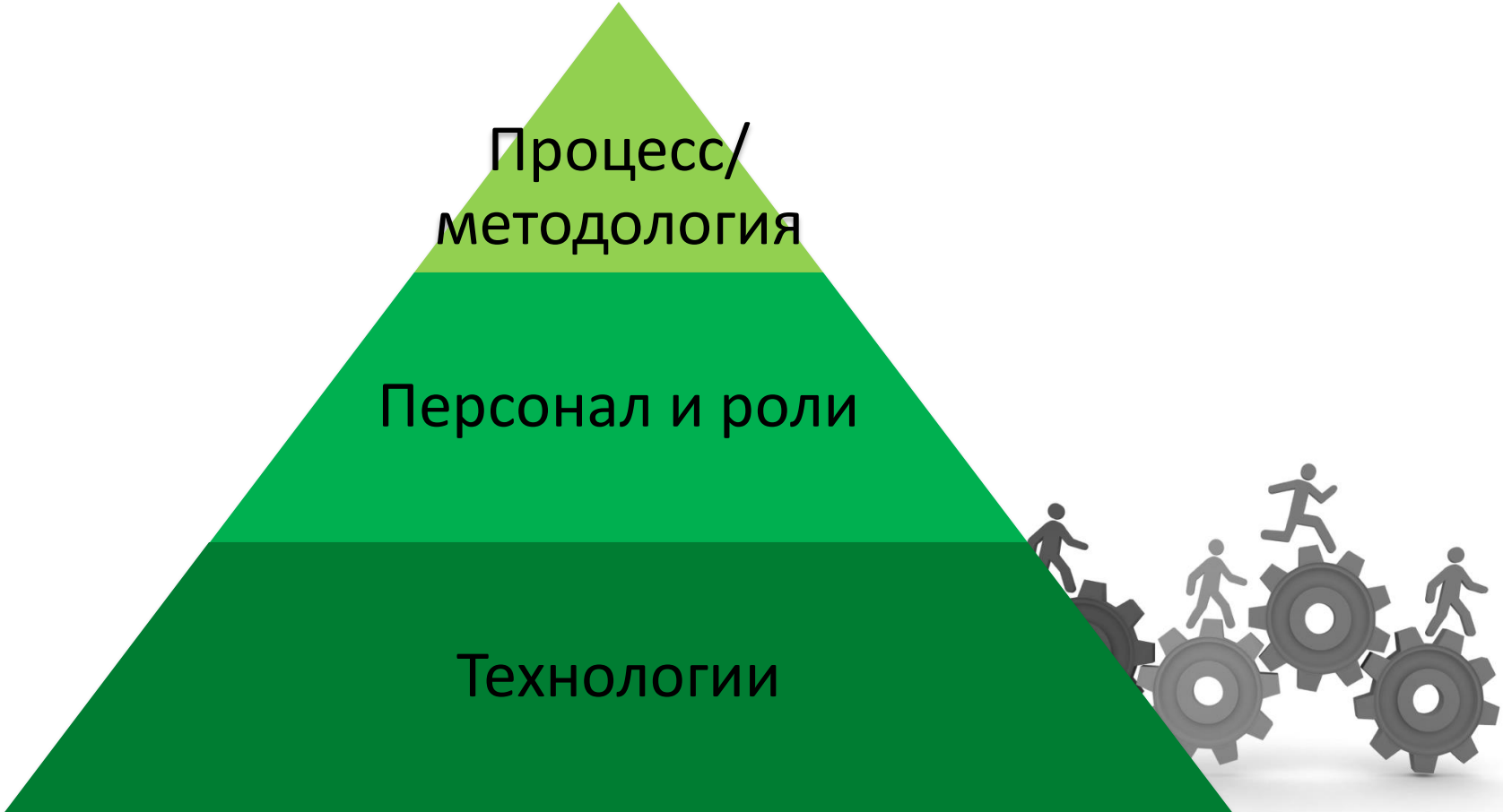
Кадровые угрозы

Коррупционные проявления, сговоры, мошенничество

Нарушение внутренних регламентов, бизнес-процессов

SOC

INFOWATCH®



SOC = СЗИ/лог-файлы

DLP = люди/контент

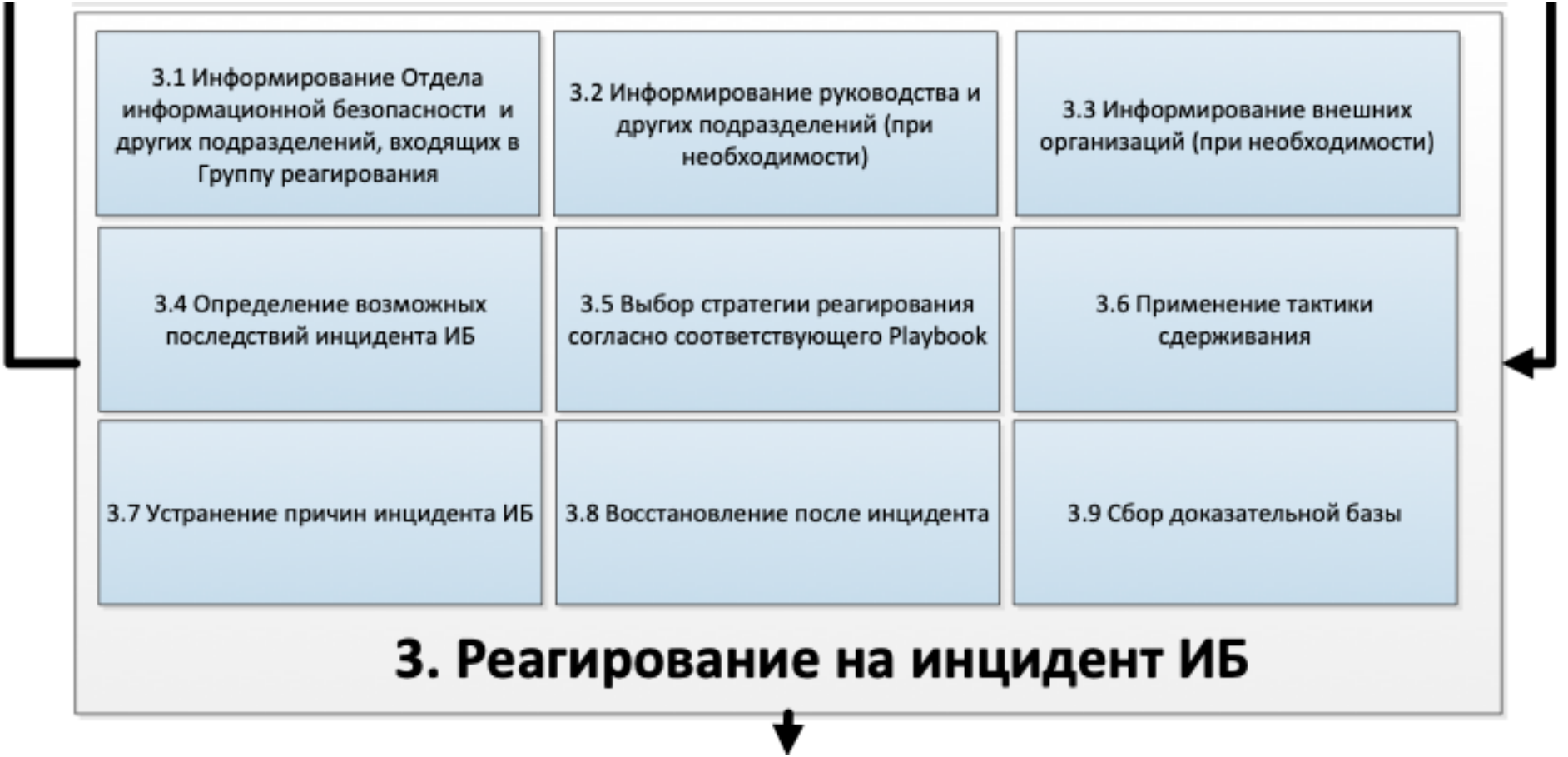
Этапы реагирования на инциденты (1)

INFOWATCH®

Этапы реагирования на инциденты (2)

Этапы реагирования на инциденты (3)

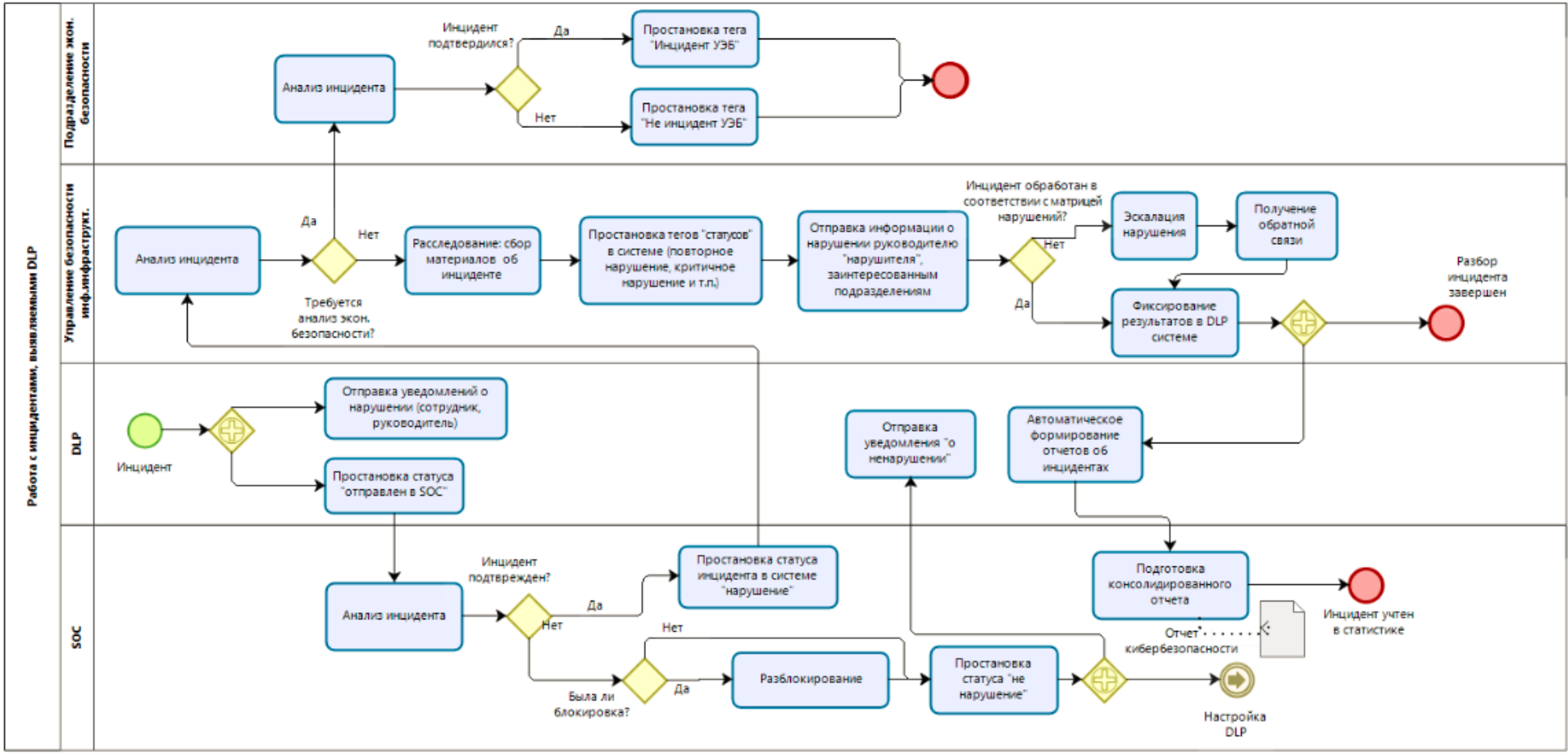
INFOWATCH®



Этапы реагирования на инциденты (4)

Подружить процессы?

INFOWATCH®

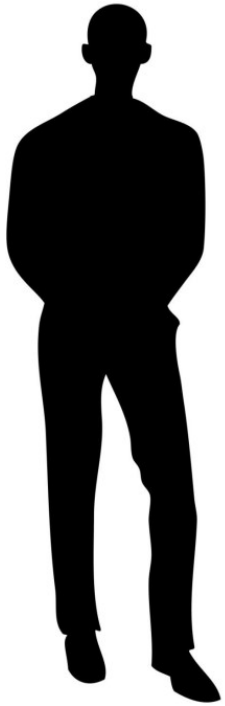


Вопрос 1. Линии реагирования – кто должен обрабатывать события из DLP?

L1 Первичная обработка событий ~~DLP~~

L2 Анализ и принятие решений ~~DLP~~

L3 Реагирование **DLP!**



RACI-матрица

INFOWATCH®

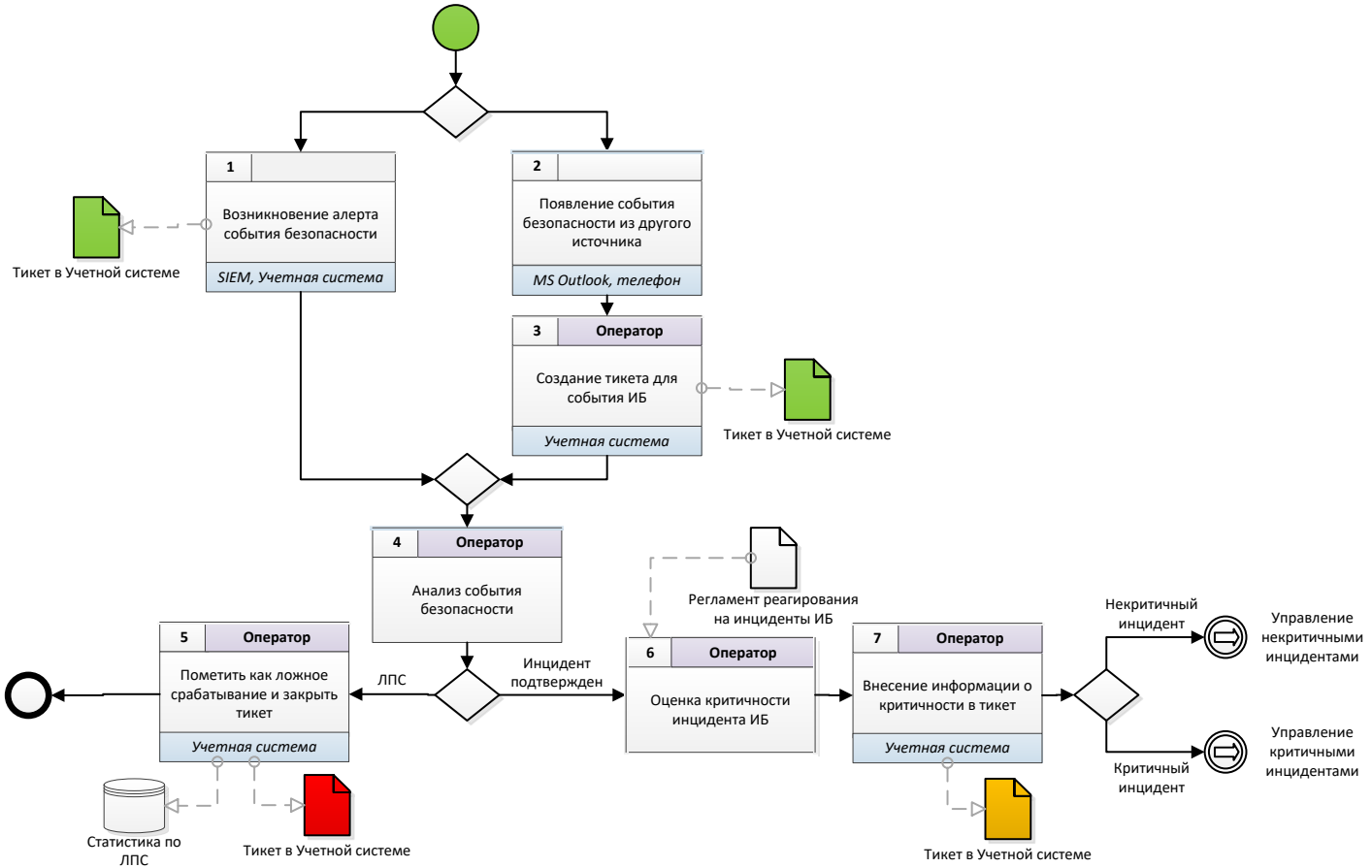
		ОИБ	Оператор L1	Аналитик L2	Группа реагирования
1.	Планирование и подготовка	A	I	R	
2.	Мониторинг и подтверждение	I	RA	C	
3.	Реагирование на некритичный инцидент ИБ – есть Playbook	RI	RA	I	
4.	Реагирование на некритичный инцидент ИБ – нет Playbook	RA	C	RA	
5.	Реагирование на критичный инцидент ИБ	R		C	A
6.	Анализ причин и планирование улучшений	CI	C	RA	

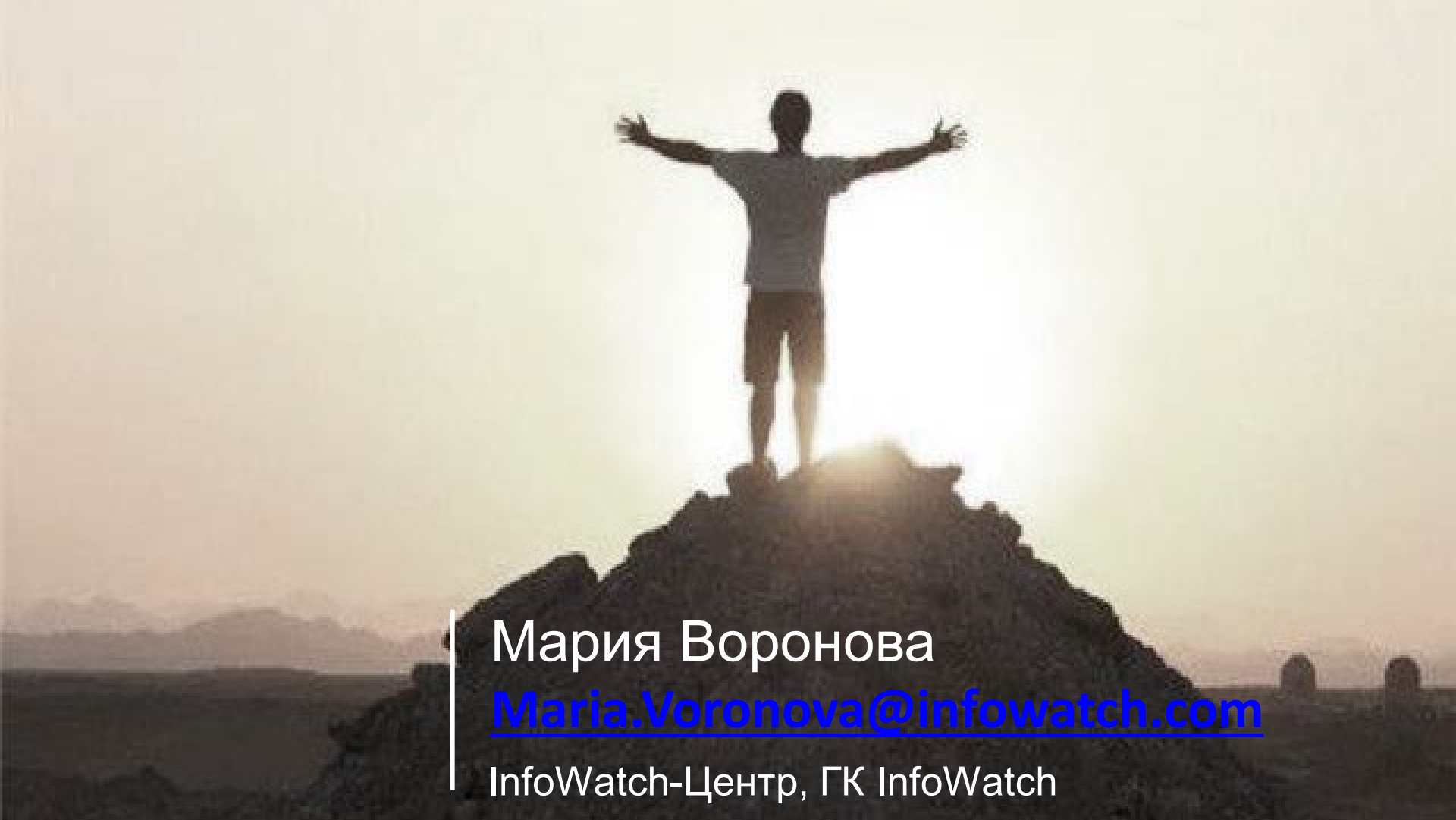
Вопрос 2. Критерии обработки событий

Класс инцидента	Описание	Ответственное за рассмотрение подразделение
Инциденты внутренней безопасности	Инциденты, характеризующиеся наличием умысла и имеющие признаки экономических нарушений и мошеннических действий.	Внутренняя безопасность
Формальные инциденты	Инциденты, имеющие формальные признаки нарушения при отсутствии ущерба и умысла.	SOC
	Инциденты, имеющие формальные признаки нарушения с возможным причинением ущерба при отсутствии признаков умысла, а также признаки рецидива.	ОИБ
Инциденты с неустановленными параметрами	Инциденты, у которых не установлены необходимые для их дальнейшей обработки признаки (ущерб, умысел, причины, обстоятельства, заинтересованные и/или причастные лица).	Руководство ОИБ

Вопрос 3. Эффективность/KPI

Процесс «под ключ»





Мария Воронова
Maria.Voronova@infowatch.com
InfoWatch-Центр, ГК InfoWatch