

SOC Day 2019



МАРИЯ ВОРОНОВА

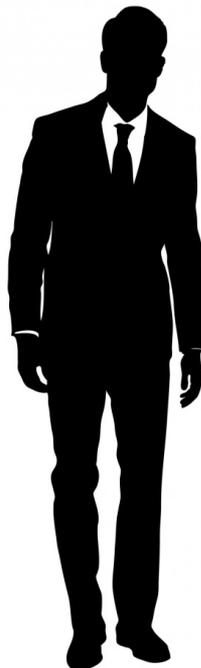
Методики и процессы внутри SOC при реагировании на инциденты утечки информации

InfoWatch-Центр, ГК InfoWatch

Актуальное инсайдерство

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

Коррупционные проявления, сговоры, мошенничество



Нелояльное поведение работников, саботаж

Кадровые угрозы

Нарушение внутренних регламентов, бизнес-процессов

Процесс/
методология

Персонал и роли

Технологии



SOC = СЗИ/лог-файлы

DLP = люди/контент



Этапы реагирования на инциденты (1)



Этапы реагирования на инциденты (2)



2.1 Сбор событий ИБ

2.2 Обнаружение инцидента ИБ

2.3 Подтверждение инцидента ИБ

2.4 Определение подверженных инциденту ИБ информационных ресурсов и процессов

2.5 Оценка критичности инцидента ИБ

2.6 Регистрация инцидента ИБ (создание тикета в учетной системе)

2. Мониторинг и подтверждение инцидента ИБ

Этапы реагирования на инциденты (3)



4.1 Документирование, в том числе отчет по инциденту ИБ

4.2 Закрытие тикета в учетной системе

4.3 Организация хранения свидетельств, результатов, отчетность по событиям и инцидентам ИБ

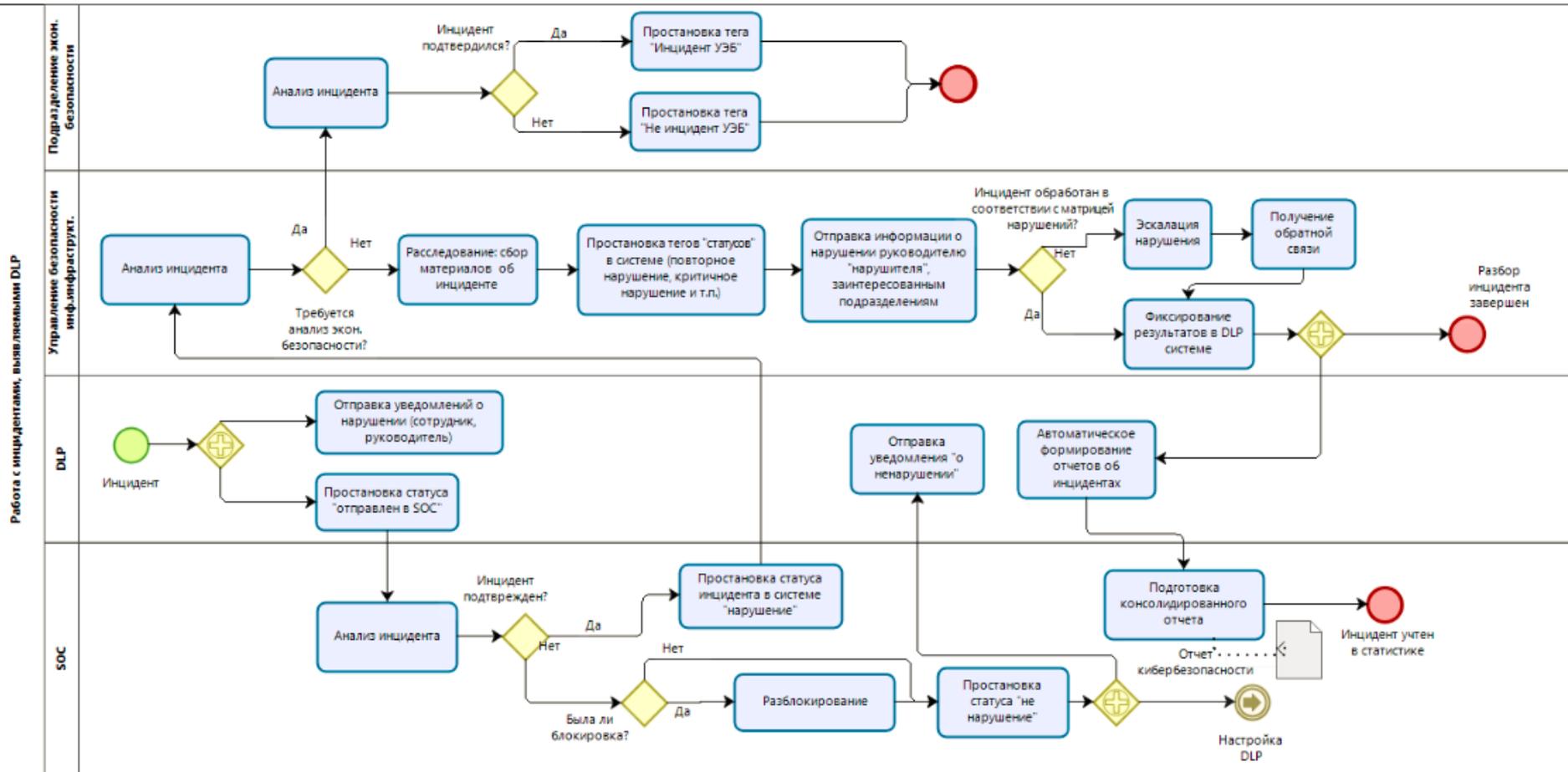
4.4 Определение причин и последствий инцидента ИБ/ложного срабатывания

4.5 Составление рекомендаций по улучшению процесса управления инцидентами ИБ

4.6 Пересмотр процедур реагирования на инциденты ИБ

4. Анализ причин и планирование улучшений

Подружить процессы?



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

L1

Первичная обработка событий

~~DLP~~

L2

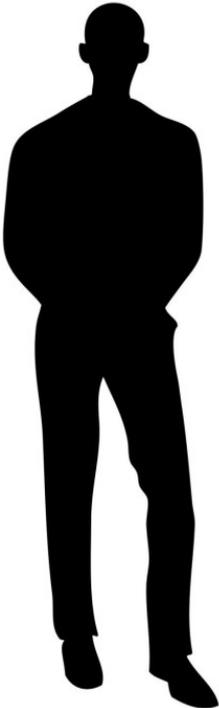
Анализ и принятие решений

~~DLP~~

L3

Реагирование

DLP!



RACI-матрица

		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

KPI 1. Выявление инцидентов

Больше чем **95% событий**, выявляемых DLP системой, подтверждены в качестве инцидентов

KPI 2. Реагирование на инциденты

Время реакции (принятия решения) по инциденту – **4 часа** с момента выявления DLP системой

KPI 3. Реагирование на события блокировки

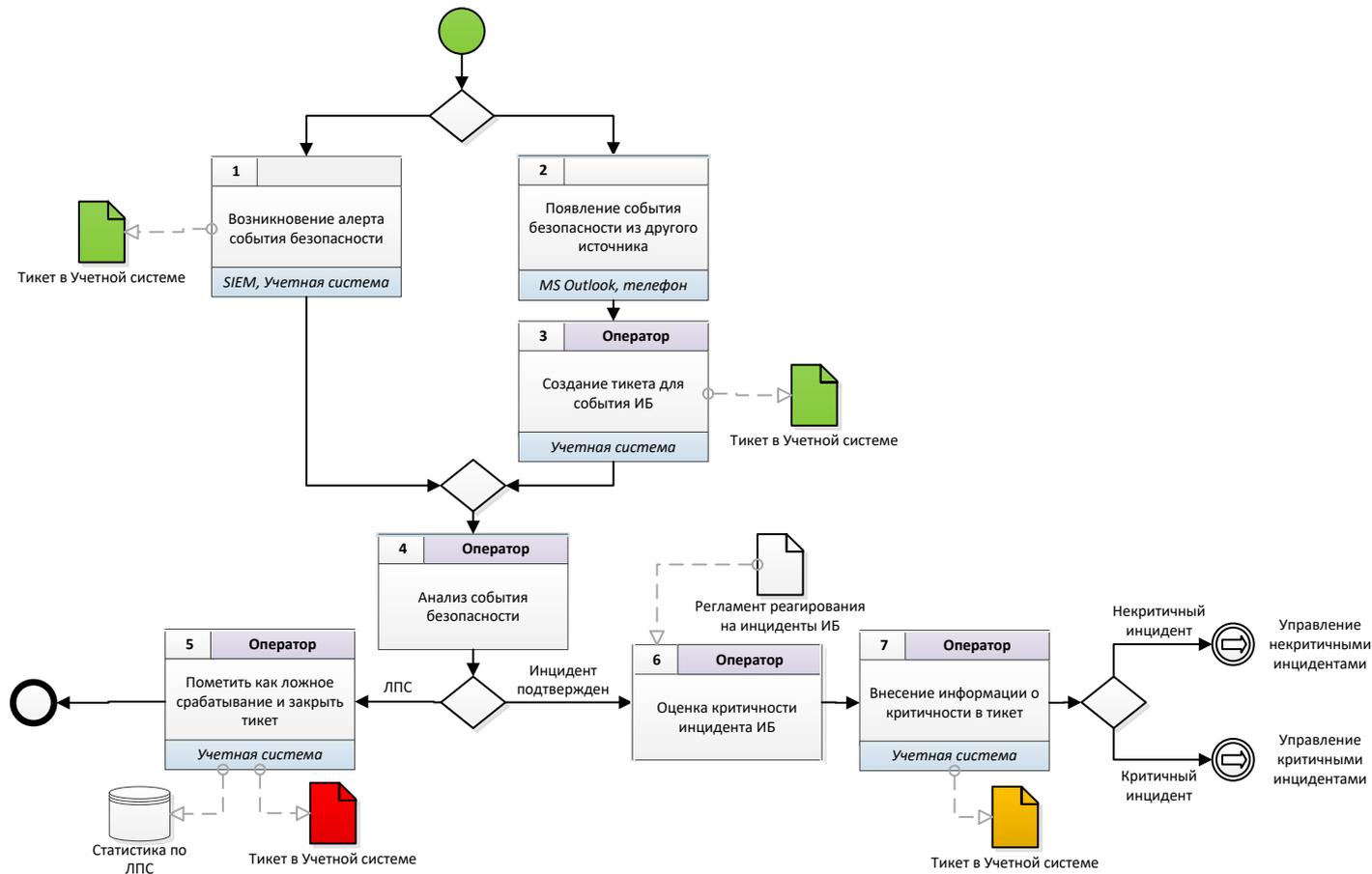
Время реакции (принятия решения) по инциденту – **не более 15 минут** с момента блокировки

KPI 4. Расследования и результат

Не менее **90% инцидентов** высокого уровня доведены до принятия управленческого решения

Ключевые показатели
эффективности
процесса

Процесс «под ключ»





Мария Воронова

Maria.Voronova@infowatch.com

InfoWatch-Центр, ГК InfoWatch