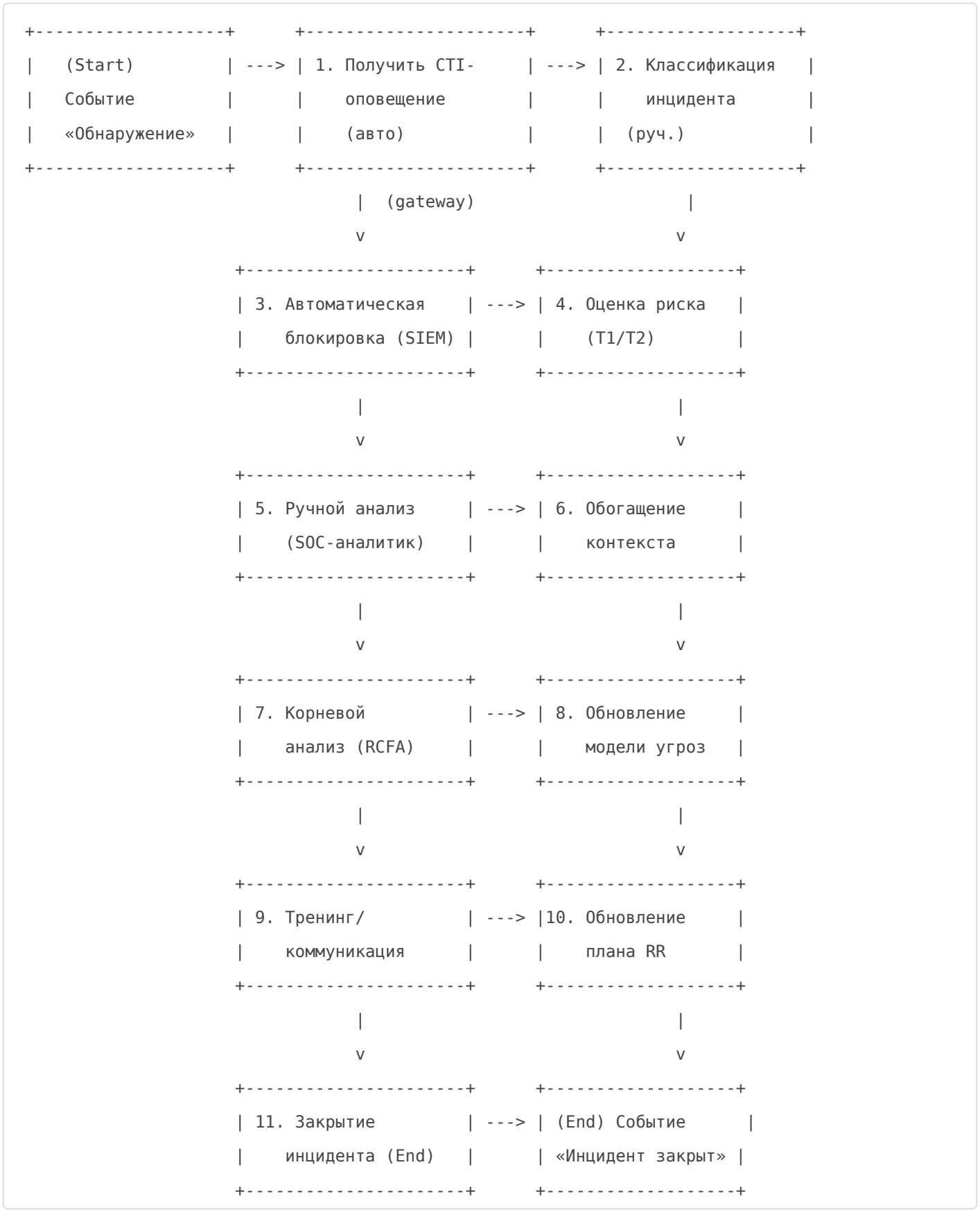
DFI: ??????? ????????????? ?? ????????

???????? ???????????? ?? ????????

1. **Анализ причин (Root-cause analysis)**
   - Сначала выясняем, что именно привело к утечке данных.
   - Составляем список недостающих мер контроля и разрабатываем план, как избежать подобных проблем в будущем.
   - Ключевые вопросы: какие-то меры предотвращения угроз не были применены? Каков был доступ (внешний / внутренний) к системе?
2. **Обновление базовой модели угроз**
   - На основании новой информации меняем уровни опасности для конкретных злоумышленников и пересматриваем профиль угроз для затронутых систем.
   - При необходимости внедряем новые механизмы обнаружения, чтобы лучше ловить похожие атаки.
3. **Оценка человеческого фактора**
   - Анализируем, могла ли ошибка сотрудника стать причиной инцидента.
   - Если да – планируем и проводим тренировку по повышению осведомлённости пользователей (фишинг, безопасная работа с данными и т.д.).
4. **Обогащение контекста оповещения/инцидента**
   - Проверяем, какие данные были упущены на каждом этапе обработки CTI-оповещения и инцидента.
   - Особое внимание уделяем шагам, где происходил обмен информацией между командами.
   - Планируем улучшения, чтобы в следующий раз весь необходимый контекст был доступен сразу.
5. **Обновление плана реагирования**
   – На основе выявленных недостатков вносим правки в текущие процедуры и сценарии реагирования (добавляем новые шаги, меняем порядок действий).

---

1. ????? (BPMN??????????) ??????? 1 – «?????? ????????? ???? ?????????»



- **Стрелки** – переходы потока.
- **(gateway)** – точка принятия решения (одно-или многопутевой шлюз).
- **(авто)** – автоматизированный шаг (скрипт, SIEM-правило).
- **(руч.)** – действие, требующее участия аналитика.

- **T1/T2** – типы задач в соответствии с инструкциями (см. таблицу 2).

Эта схема построена на описанных в приложении элементах диаграмм: начальное и конечное событие, задачи (автоматизированные и ручные), шлюзы и вспомогательные процедуры [1].

---

2. ?????????1. ???????? BPMN ?????????? ? ?? ???????????? ????????

Элемент	Тип BPMN	Техническое назначение	Пример применения в сценарии
Событие (начальное)	Event (Start)	Триггер, инициирующий процесс (получение CTI-оповещения, обнаружение аномалии в SIEM).	«Обнаружение подозрительного размещения данных».
Событие (конечное)	Event (End)	Завершение процесса, фиксирование статуса инцидента.	«Инцидент закрыт».
Задача (автоматизированная)	Task (Service)	Выполняется скриптом/правилом SIEM, SOAR, API-интеграцией.	Автоматическая блокировка IP-адреса.
Задача (ручная)	Task (User)	Операция, требующая человеческого вмешательства (анализ логов, интервью с владельцем бизнес-процесса).	Ручной анализ утечки в SOC.
Задача T1/T2/T3	Task (Manual)	Специфические задачи, привязанные к инструкциям (например, T1 – первичная оценка, T2 – детальный RCFA).	Задача T2 – корневой анализ причины.
Задача, назначенная аналитику	Task (User)	Операция, явно распределённая конкретному сотруднику (через тикет-систему).	Тикет «RCFA-2026-04-06-001» назначен старшему аналитика.
Шлюз (один путь)	Exclusive Gateway	Выбор единственного ветвления на основе условия (например, “риск > high → эскалация”).	Если уровень риска = high → перейти к задаче 8.

Элемент	Тип BPMN	Техническоеназначение	Пример применения в сценарии
Шлюз (много путей)	Parallel Gateway	Параллельное выполнение нескольких веток без приоритета.	Одновременно запускать задачи 7 и 9.
Вспомогательная процедура	Sub-Process	Выделенный под-процесс, «свернутый» в диаграмме, выполняющий поддерживающие действия (например, «Формирование отчёта о вредоносном файле»).	Подпроцесс «Отчёт по DDoS-атаке».

Все определения взяты из приложенного файла [1].

---

3. ??????????2. ??????????? ?????? ????? ? ????????????? ????????

№	Наименование задачи	Техническая реализация	Инструменты / Платформы	Выходные артефакты
1	Приём CTI-оповещения	API-получение от внешних источников (MISP, Threat-Intel-Feeds)	MISP, OpenCTI, SOAR-платформа	JSON-сообщение, тикет в ServiceNow
2	Классификация инцидента	Правило в SIEM (Splunk, QRadar) → рейтинг CVSS/EPSS	Splunk ES, QRadar IR, Cortex XSOAR	Тег «DARKWEB_LEAK», приоритет P1
3	Автоматическая блокировка	Playbook-action: блокировать IP/URL в FW, обновить deny-list	Palo Alto API, Cisco FMC, FortiGate	Запись в firewall-лог
4	Оценка риска (T1/T2)	Корреляция с бизнес-приоритетами, расчёт «impact»	ServiceNow Risk, RSA Archer	Risk-score, рекомендация по эскалации
5	Ручной анализ (SOC)	Анализ логов, поиск IOC-ов, запрос у владельцев	ELK, Graylog, Kibana, Wireshark	Аналитический отчёт (PDF)
6	Обогащение контекста	Enrichment – добавление WHOIS, Shodan, VirusTotal	VirusTotal API, PassiveTotal, Shodan	Обогащённый IOC-пакет
7	Корневой анализ (RCFA)	5-Why, Fishbone, построение тайм-лайн	Miro, Lucidchart, JIRA	RCFA-документ, диаграмма причин

№	Наименование задачи	Техническая реализация	Инструменты / Платформы	Выходные артефакты
8	Обновление модели угроз	Пересчёт ATT&CK-техник, обновление MITRE-ATT&CK matrix	ATT&CK Navigator, ThreatModeler	Обновлённый ATT&CK-профиль
9	Тренинг/коммуникация	Плановое обучение, рассылка «lessons learned»	KnowBe4, LMS, Teams	Протокол обучения, feedback-форма
10	Обновление плана реагирования (RR)	Версионирование плана в Git, CI/CD-тестирование	GitLab, Confluence, Ansible	New-RR-v2.3 (PDF)
11	Закрытие инцидента	Финальный тикет-статус = «Closed», пост-мортем-рекомендации	ServiceNow, JIRA, Confluence	Пост-мортем-отчёт, KPI-отчёт

4. ??????????? ????? ?????? (Data Flow Diagram – ????????2)

Степень	Источник / Приёмник	Путь передачи	Формат / Протокол	Описание
1	Внешний Threat-Intel-Feed	HTTPS POST → SIEM	JSON	Приём новых IOC-ов о публикации в дарк-вебе.
2	SIEM → SOAR	REST API	JSON	Триггер автоматической блокировки и создания тикета.
3	SOAR → Firewall	API (XML/JSON)	HTTPS	Добавление IP/URL в deny-list.
4	SOC-аналитик → Wiki	Web-UI	HTML/Markdown	Документирование анализа и выводов.
5	Wiki → Threat-Modeling tool	Export/Import	CSV/JSON	Обновление модели угроз на основе новых тактик.
6	Training platform → End-users	SMTP / LMS portal	HTML-email	Рассылка обучающих материалов.

Степень	Источник / Приёмник	Путь передачи	Формат /Протокол	Описание
7	RR-repository (Git) → CI/CD	Git push/pull	Git	Автоматическая проверка синтаксиса и публикация новой версии.

---

5. ?????????? ? ?????????????? ?????? (gateways)

Шлюз	Логика	Техническая реализация
Exclusive Gateway	`if (risk_score >= 80) → путь A (эскалация)` `else → путь B (детальный анализ)`	BPMN-правило в Camunda (`${riskScore >= 80}`)
Parallel Gateway	Запуск **задач 7 и 9** одновременно, без ожидания завершения первой	`parallelGateway` в BPMN-модели, распределяем поток в два подпроцесса

---

6. ?????? ?????????????? (SOAR? playbook) ??? ????????3 « ?????????????? ??????????»

```
# playbook.yaml — Cortex XSOAR
id: block_darkweb_ioc
name: Block IOC from DarkWeb leak
tasks:
  - name: Get IOC from incident
    script: GetIncidentIOC
    output:
      - ioc_ip
  - name: Add to firewall deny-list
    script: PaloAltoBlockIP
    args:
      ip: ${ioc_ip}
```

```
    condition: ${ioc_ip} != None
  - name: Update ticket status
    script: UpdateTicket
    args:
      status: "In Progress"
```

Этот playbook реализует **автоматизированную задачу** (см. элемент «Задача Действие интеграции, которое может быть автоматизировано» в таблице 1) [1].

??????????

Схема, таблицы и примеры кода выше дают **техническое** представление о полном жизненном цикле реагирования на утечку данных в дарк-вебе, используя строго определённые элементы BPMN-диаграмм (начальное/конечное событие, задачи, шлюзы, вспомогательные процедуры) и интеграцию с реальными системами SOC/SIEM/SOAR [1]. При необходимости любую из ветвей (например, более детальный RCFA или автоматизацию блокировок) можно расширить отдельными под-процессами, сохраняя совместимость с текущей схемой.

Revision #2
Created 6 April 2026 12:46:32 by Administrator
Updated 6 April 2026 13:40:59 by Administrator