USSC

Автоматизация SecOps: IRP/SOAR

Екатеринбург, 22.02.2022

Что такое SOAR, IRP и SGRC?

В чём выгода?

Действие	До SOAR	SOAR	Пример
Эскалация через SIEM, EDR или NGFW	5 мин	10 сек	Эскалация инцидента из SIEM – подозрительная активность на рабочей станции
Идентификация активов – CMDB/AD/IAM	5-10 мин	10 сек	Запросы в CMDB по рабочей станции и в Active Directory по пользователю
Проверка IOC в Threat Intelligence базах	5 мин	10 сек	В инциденте есть hash связанный с ВПО
Историческая корреляция инцидентов	10-20 мин	мгновенно	2 других инцидента за последний месяц имеют тот же hash и исходящий траффик
Ручное обогащение – активности с рабочих станций, внутренней сети, логи VPN, DNS записи, сетевая инфраструктура	30-55 мин	30 сек	Используем EDR решение чтобы получить всю информацию с рабочей станции. DNS с web proxy для выявления сервера управления
Записи по инциденту – детальные записи и задачи на протяжении всего инцидента	неизвестно	мгновенно	ePlat4m автоматически сохраняет все выполненные задачи и действия по реагированию, все записи аналитиков хранятся на платформе
Эскалация через SIEM, EDR или NGFW	неизвестно	мгновенно	Все действия дотируются в ePlat4m и не могут быть модифицированы. При разборе инцидента руководство может анализировать отчеты
Отчет по статусу инцидента и визуализация для руководства	неизвестно	мгновенно	Встроенные консоли для руководства и внешние уведомления предоставляют всю информацию в режиме реального времени без лишней работы
Итого	**85 минут**	**1 минута**	

Пример автоматизации действий

При обнаружении передачи учетной записи работника другому работнику:

- Пользователь автоматически добавляется в группу недобросовестных юзеров
- Блокируется учетная запись
- Пользователю направляется уведомление с запросом получения объяснительной
- После получения объяснительной информация передаётся администратору для принятия решения о разблокировке учетной записи

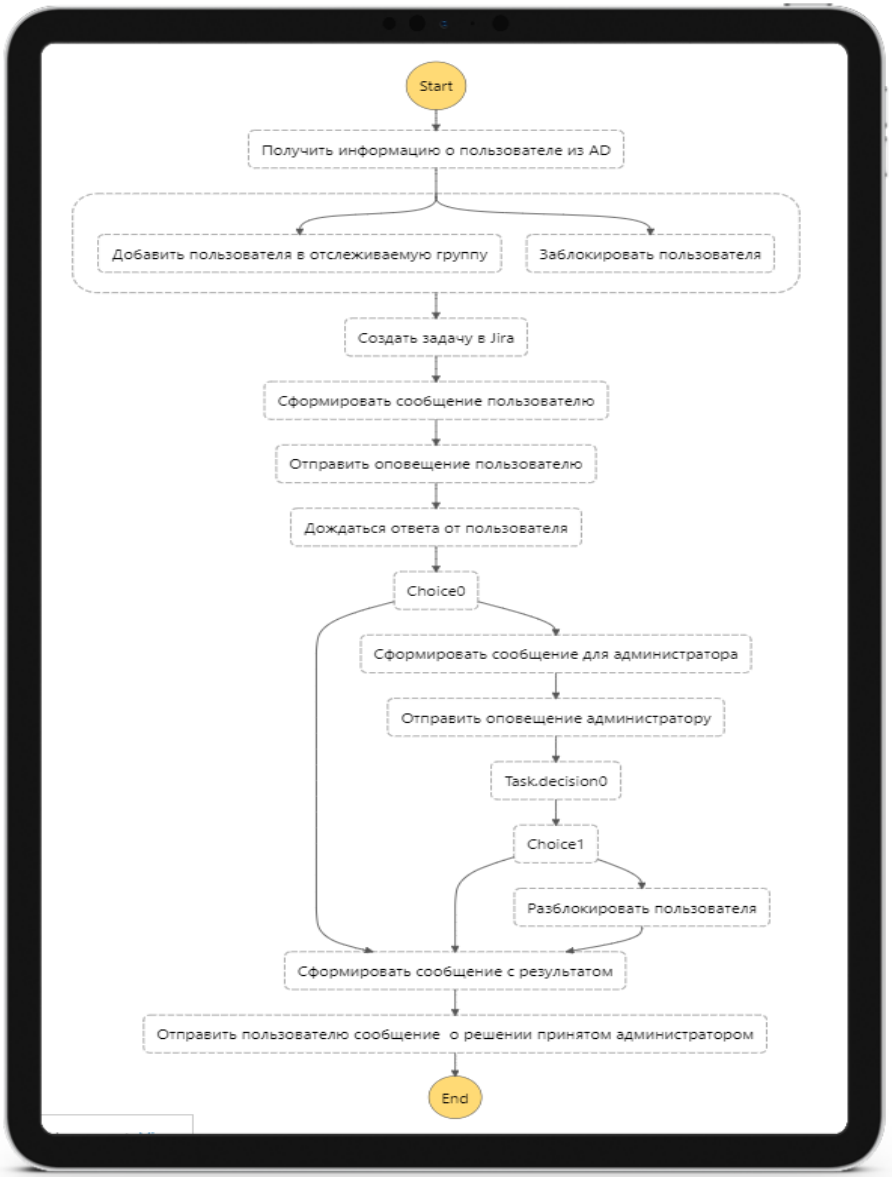
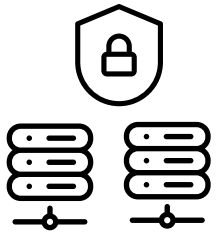


Схема работы



СрЗИ/SIEM

Инциденты

Обогащение

Threat Intelligence

Проверка IoC

ITSM

Инциденты

Задачи

Администри-рование

- Управление пользователями
- Аутентификация и авторизация
- Мониторинг и контроль

Оркестровка и автоматизация

- Коннекторы к СрЗИ, IAM, CMDB
- Плейбуки
- Скрипты

Управление реагированием

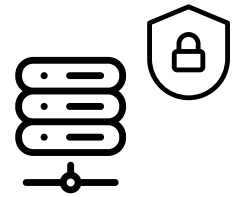
- Обработка инцидентов
- База знаний
- Отчетность

Взаимодействие

- Организация сотрудничества
- Распределение и контроль выполнения задач

Действия

Обогащение



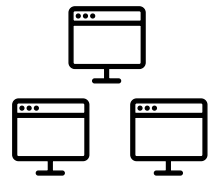
СрЗИ/IAM/ CMDB

Отчетность

НКЦКИ/ФинЦЕРТ

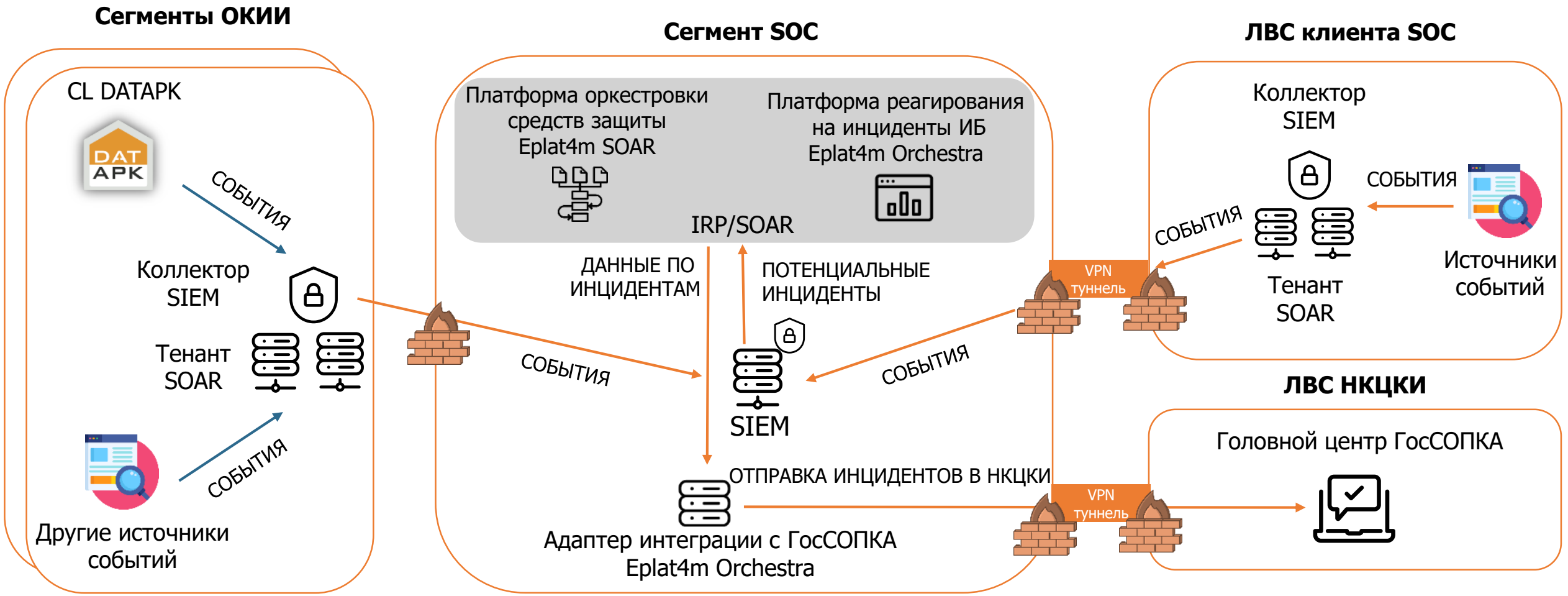
Отчетность

Инциденты



Команда SOC

Пример реальной архитектуры



Функциональная архитектура

Блок управления активами (CMDB)	Выявление активов Обогащение информации об активах
Блок управления инцидентами	Сбор сведений об инцидентах из смежных систем (SIEM) Формирование карточек инцидентов Обеспечение полного цикла расследования и реагирования Выстраивание процессов управления инцидентами
Блок реагирования	Создание и использование сценариев реагирования (плейбуков) Создание и использование скриптов автоматизации Управление расписанием Управление секретами Витрина плейбуков
Блок визуализации и отчетности	Визуализация информации: дашборды, карты, схемы, диаграммы Формирование, отображение и экспорт отчетных материалов

Инвентаризация активов

Функции:

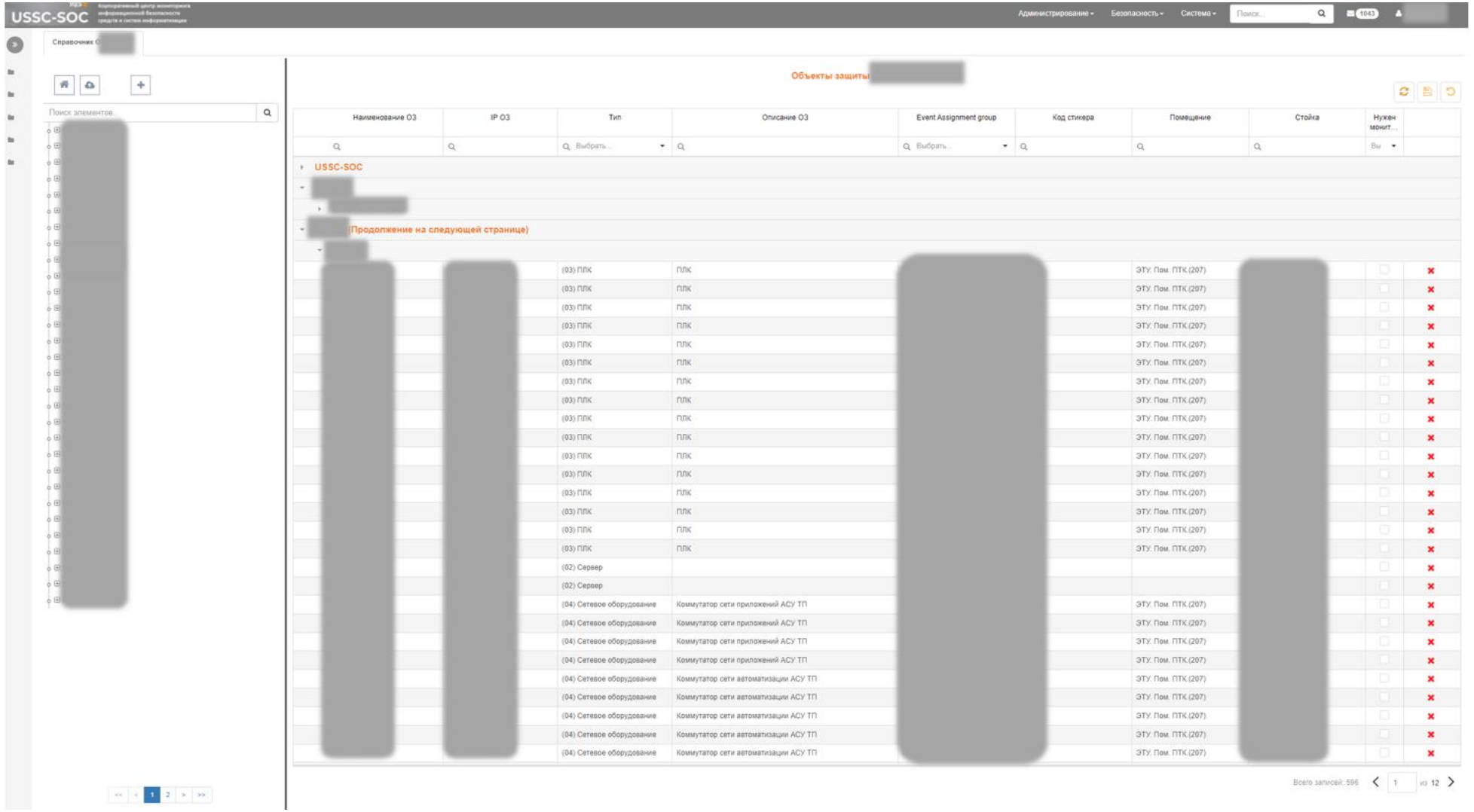
- Выявление активов
- Обогащение данных об установленном ПО, обновлениях, уязвимостях

Данные об активах собираются посредством коннекторов к:

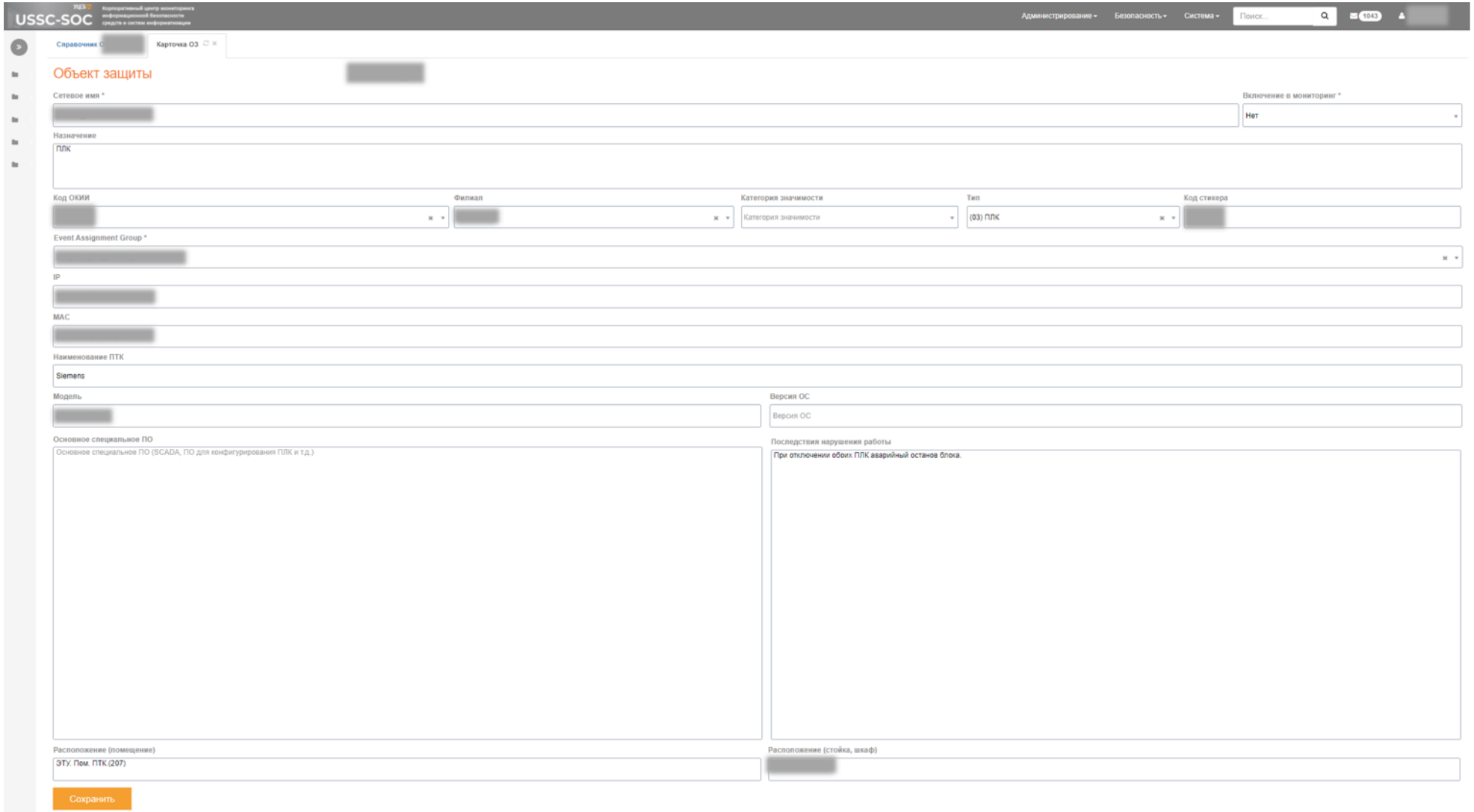
- MaxPatrol
- DATAPK
- Efros CI
- Microsoft SCCM
- Kaspersky Security Center

и другие коннекторы

Инвентаризация активов



Инвентаризация активов



Обогащение событий

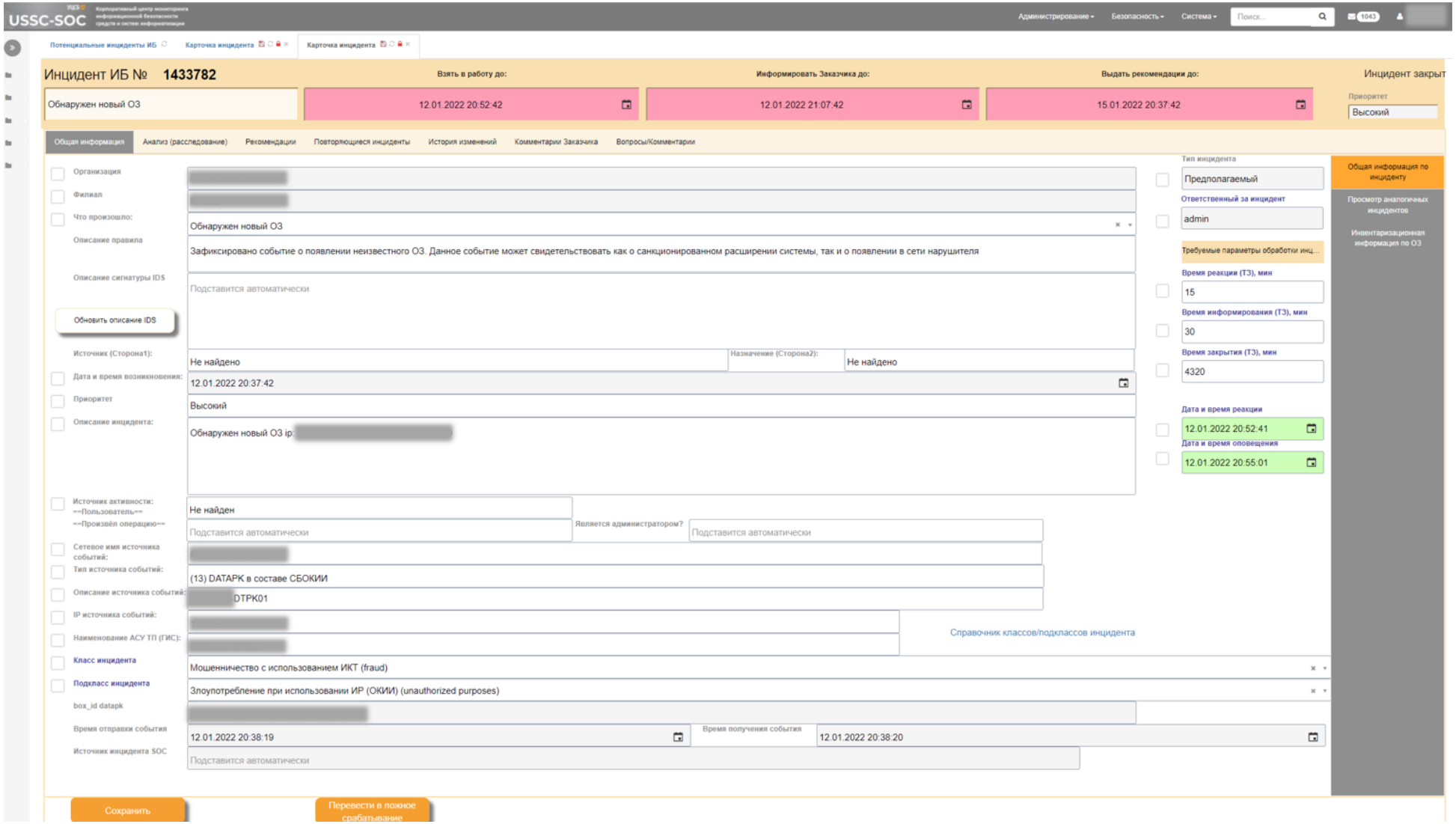
Функции:

- Обогащение данных об инциденте путем привязки дополнительной информации об объектах защиты
- Обогащение путем агрегации связанных событий безопасности
- Сбор дополнительных данных из внешних сервисов

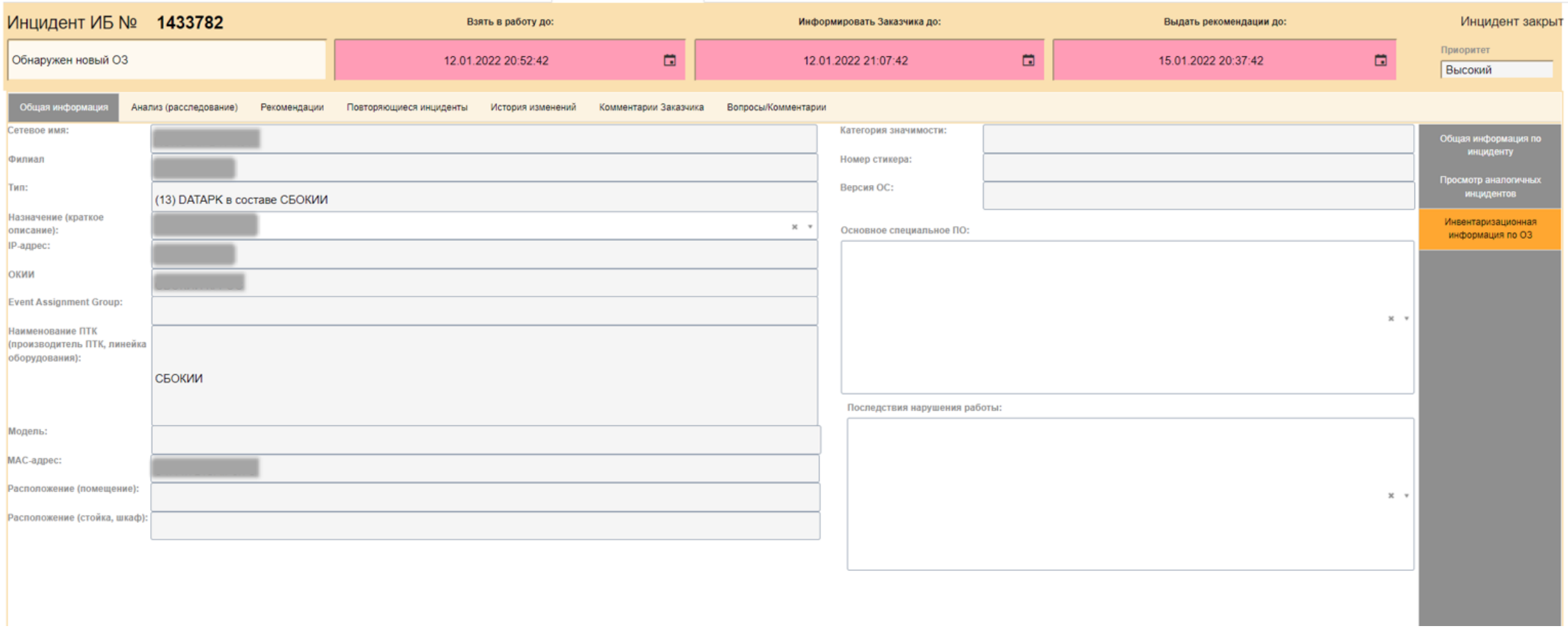
Сведения для обогащения собираются посредством коннекторов к:

- Whois
- VirusTotal
- Active Directory
- Elastic Search
- DATAPK
- Коннекторы САПУИБ

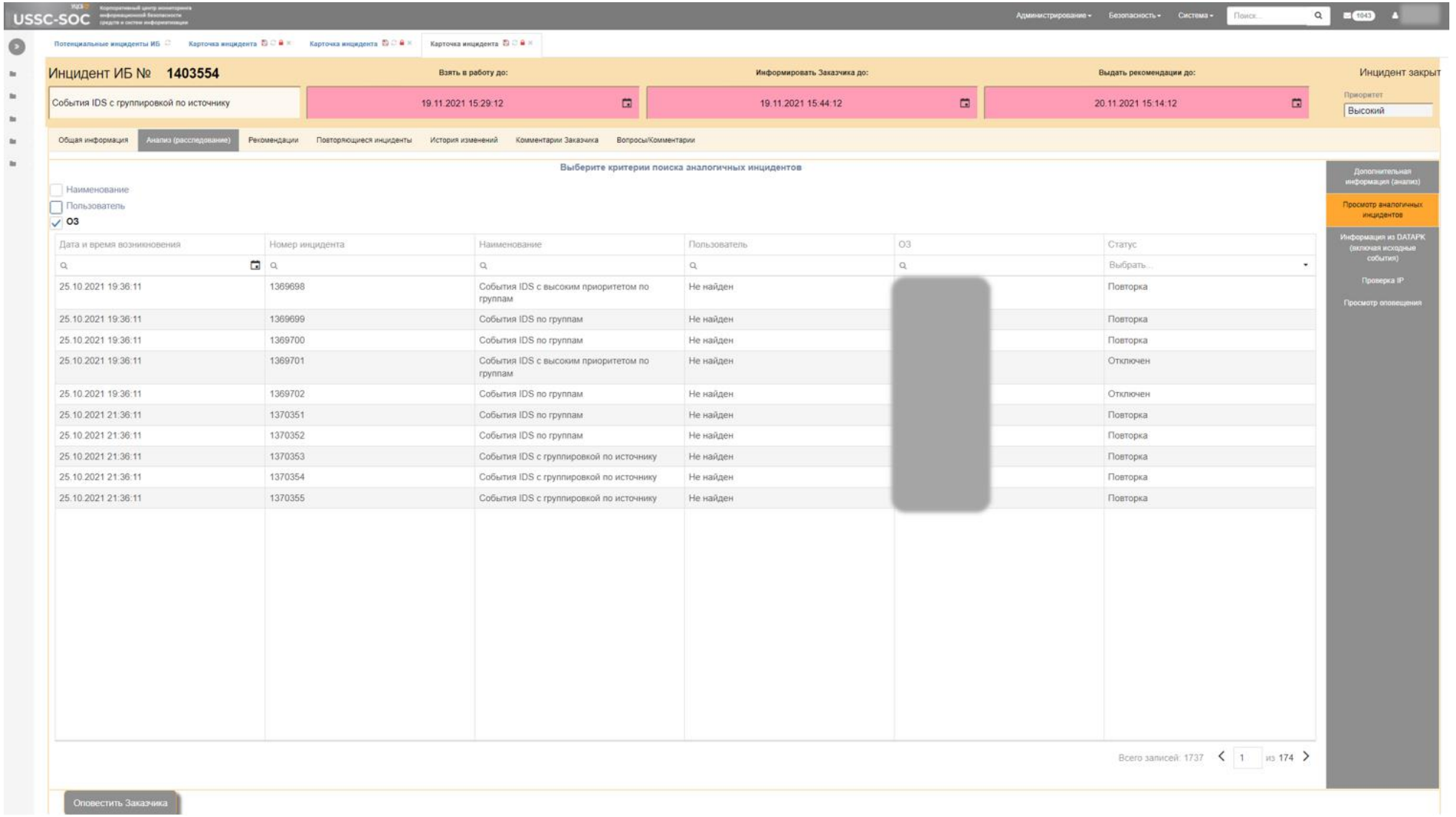
Карточка инцидента



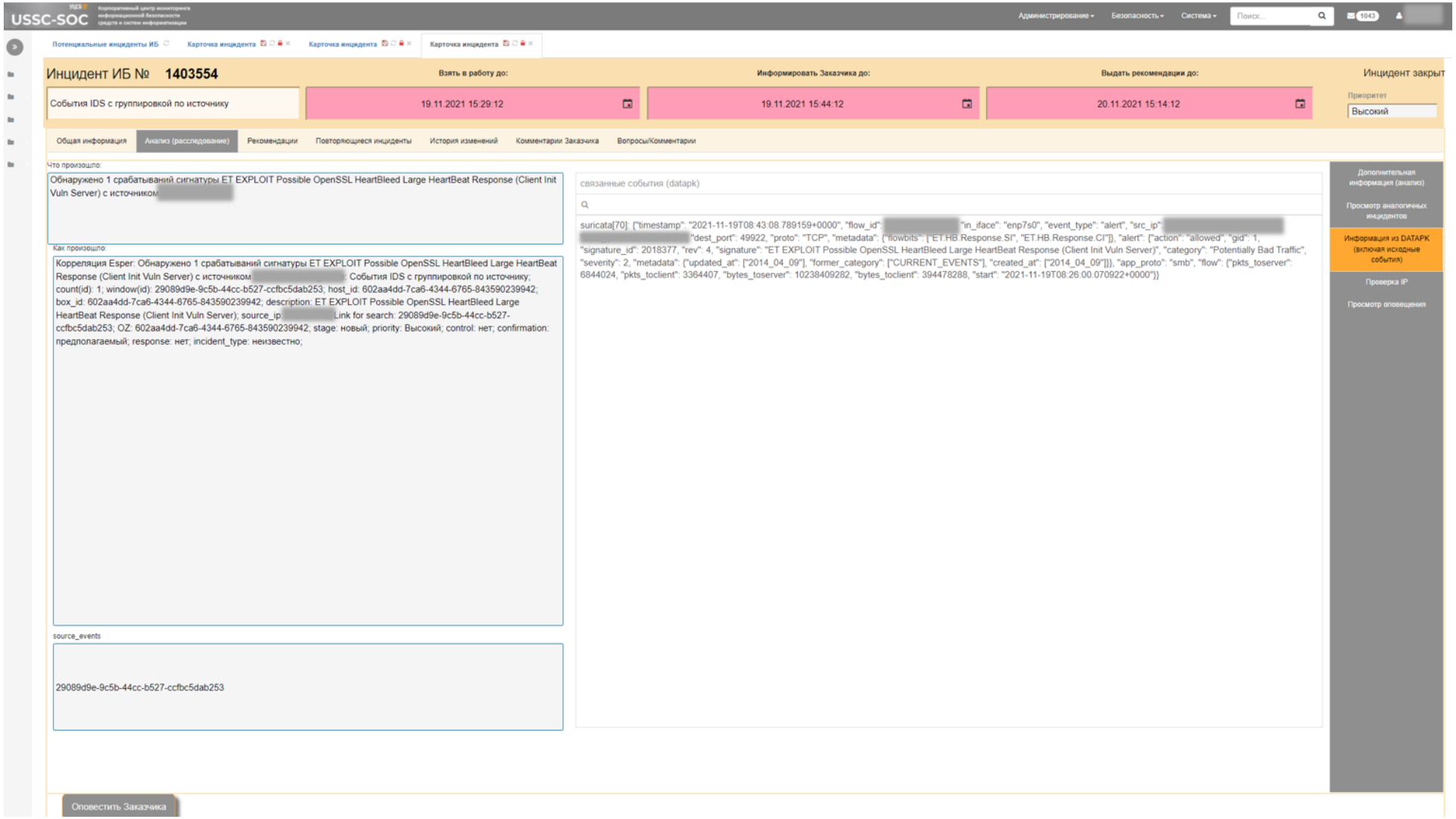
Обогащение инцидента данными из Security CMDB



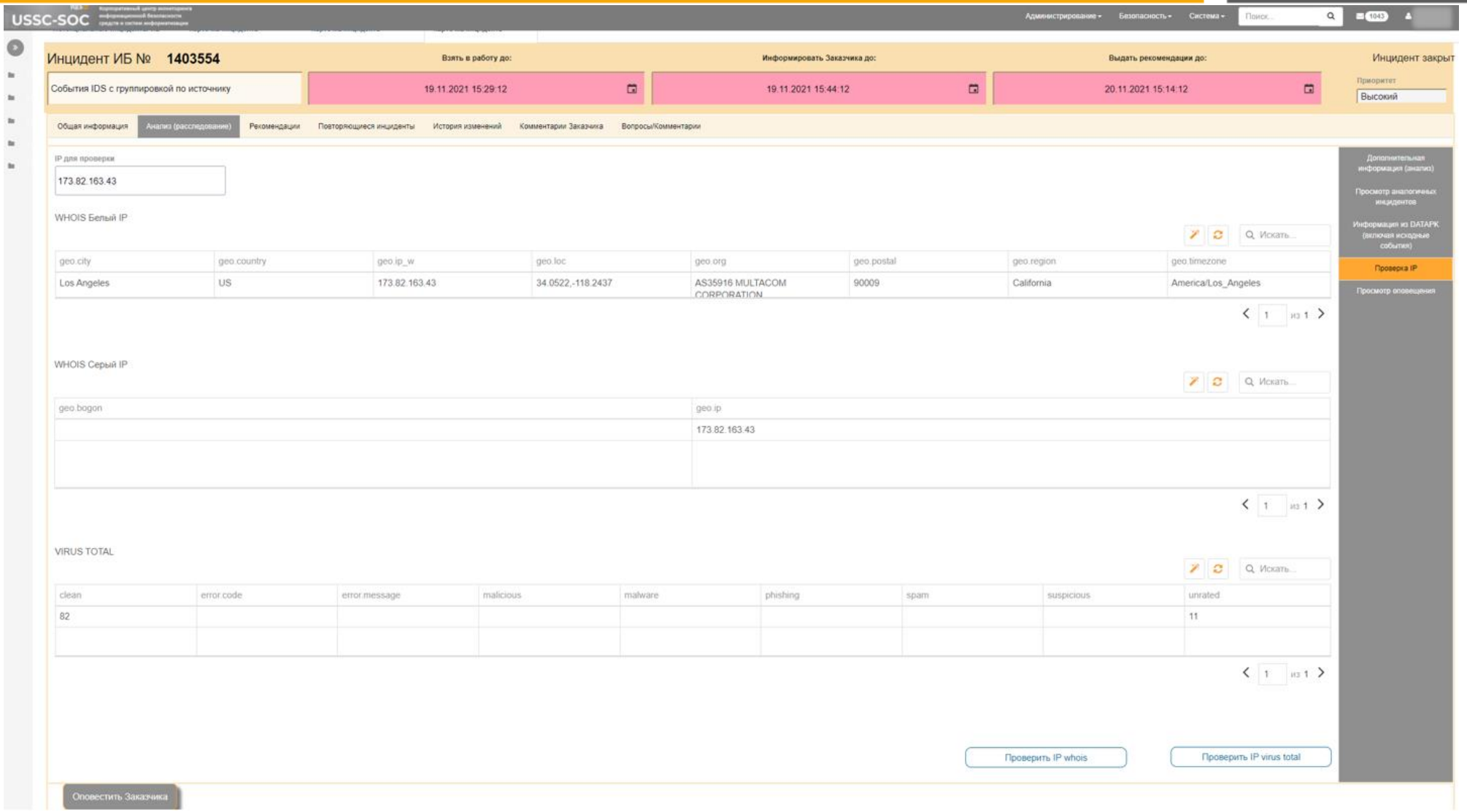
Поиск аналогичных инцидентов



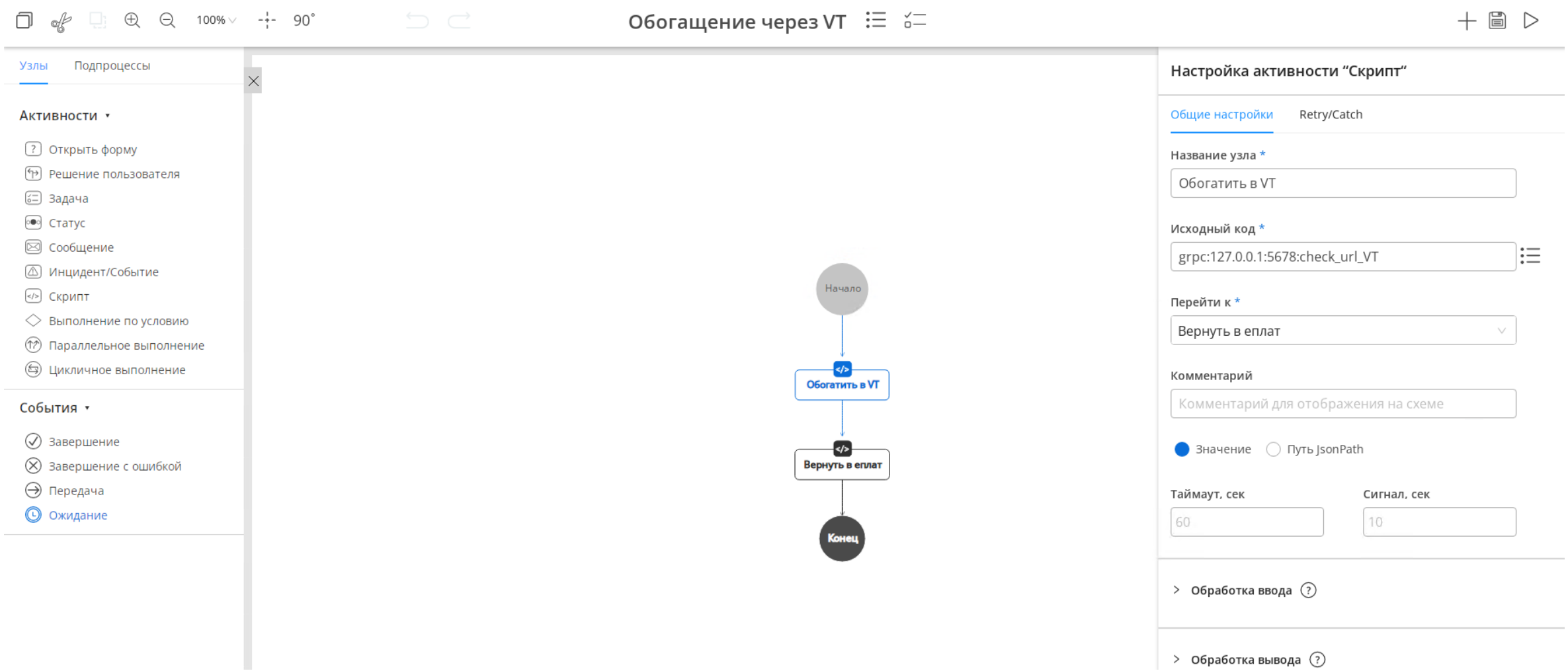
Агрегация связанных событий



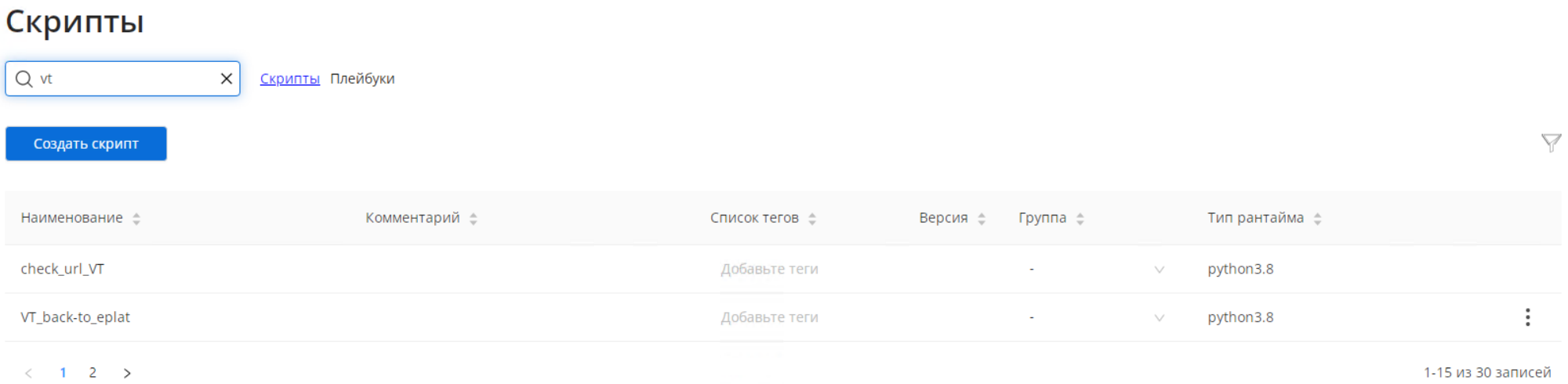
Обогащение из внешних сервисов



Плейбук обогащения инцидента на VirusTotal



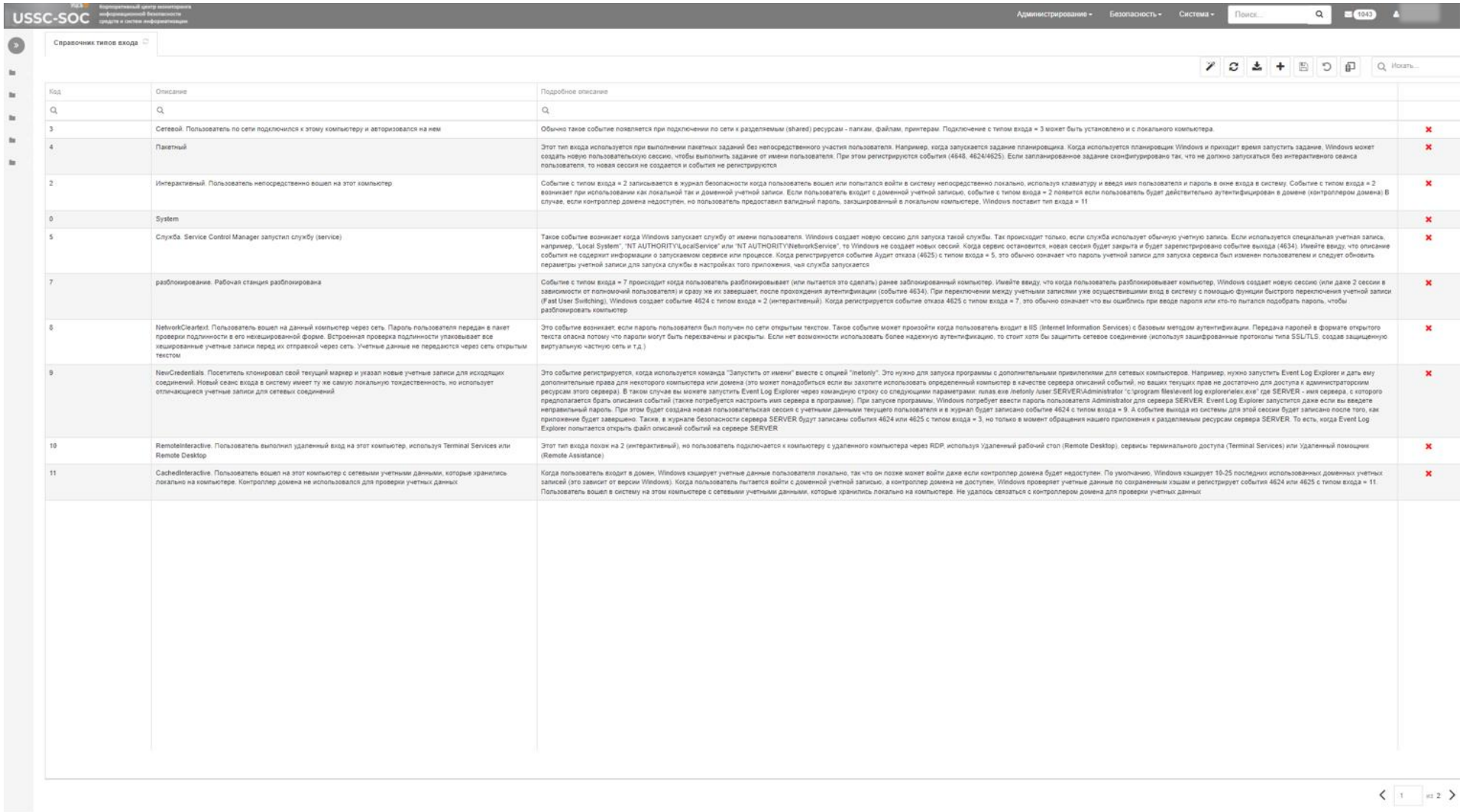
Обогащение событий – скрипты сбора данных



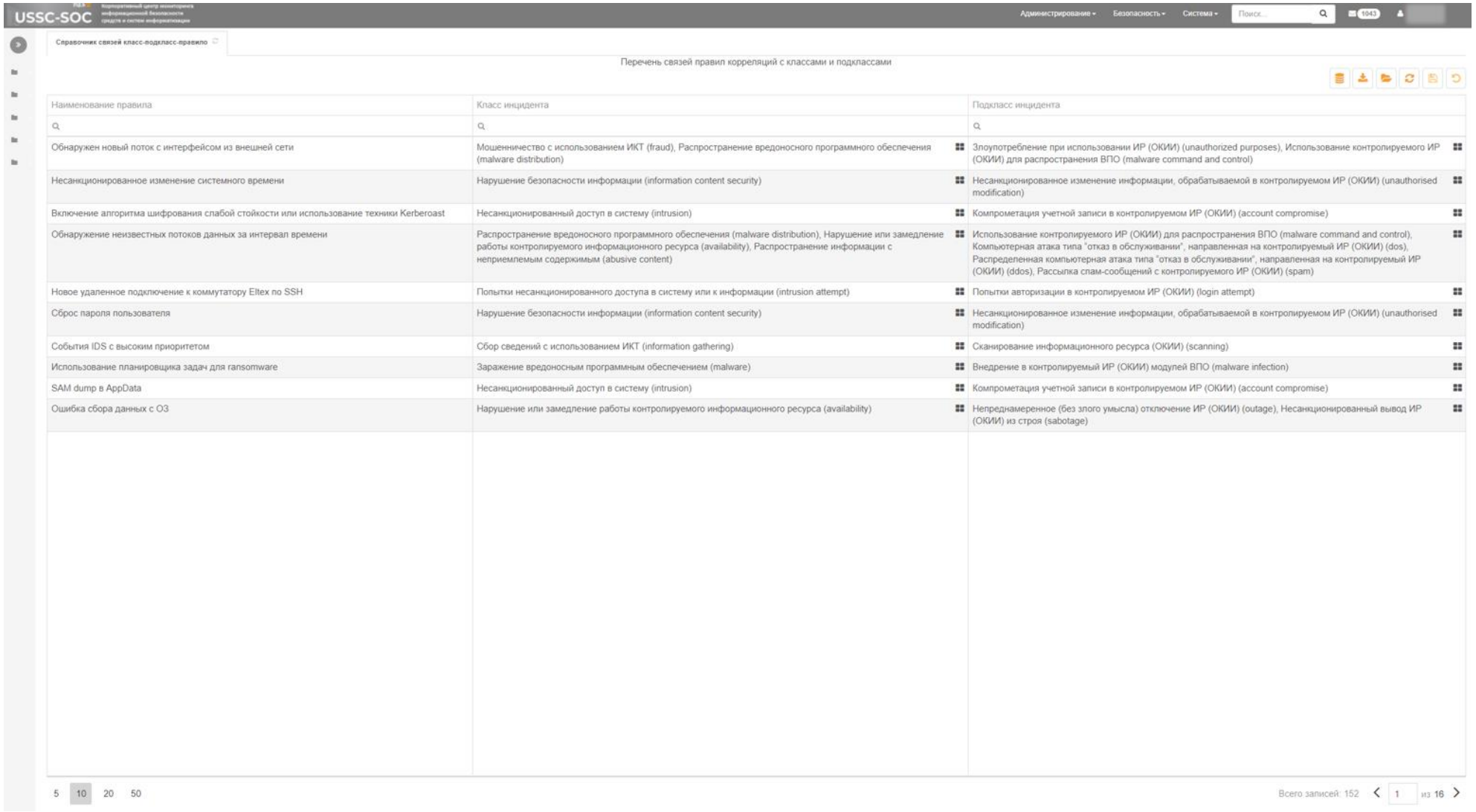
Пример скрипта сбора данных VirusTotal

```python
import json
import sys
import requests
import time


def main(input_json):
    # url = '187.1.188.158'
    url = input_json['ip']
    api_key_virustotal = input_json.get('api_key_virustotal_virustotal', [redacted])

    if 'api_key_virustotal' in input_json:
        del input_json['api_key_virustotal']

    result_counter = {}

    data = {'url': url}
    api_url = 'https://www.virustotal.com/api/v3/urls'
    headers = {'x-apikey' : api_key_virustotal}
    response_query = requests.post(api_url, headers=headers, data=data)
    if response_query.status_code != 200:
        print(json.dumps({**response_query.json(), **input_json}))
        return

    while True:
        (variable) headers: dict[str, Any]  om/api/v3/analyses/{response_query.json()["data"]["id"]}'
        headers = {'x-apikey' : api_key_virustotal}
        response = requests.get(api_url, headers=headers)
        if response.status_code == 200:
            response = response.json()
            if response['data']['attributes']['status'] == "completed":
                for i in response['data']['attributes']['results']:
                    if response['data']['attributes']['results'][i]['result'] in result_counter:
                        result_counter[response['data']['attributes']['results'][i]['result']] += 1
                    else:
                        result_counter[response['data']['attributes']['results'][i]['result']] = 1
                break
            else:
                time.sleep(2)
        else:
            time.sleep(2)

    print(json.dumps({**result_counter, **input_json}))

if __name__ == '__main__':
    input_str = sys.argv[1]
    input_json = json.loads(input_str)
    main(input_json)
```

Обогащение инцидента справочной информацией



Обогащение инцидента классами/подклассами



Наименование правила	Класс инцидента	Подкласс инцидента
Обнаружен новый поток с интерфейсом из внешней сети	Мошенничество с использованием ИКТ (fraud), Распространение вредоносного программного обеспечения (malware distribution)	Злоупотребление при использовании ИР (ОКИИ) (unauthorized purposes), Использование контролируемого ИР (ОКИИ) для распространения ВПО (malware command and control)
Несанкционированное изменение системного времени	Нарушение безопасности информации (information content security)	Несанкционированное изменение информации, обрабатываемой в контролируемом ИР (ОКИИ) (unauthorised modification)
Включение алгоритма шифрования слабой стойкости или использование техники Kerberoast	Несанкционированный доступ в систему (intrusion)	Компрометация учетной записи в контролируемом ИР (ОКИИ) (account compromise)
Обнаружение неизвестных потоков данных за интервал времени	Распространение вредоносного программного обеспечения (malware distribution), Нарушение или замедление работы контролируемого информационного ресурса (availability), Распространение информации с неприемлемым содержимым (abusive content)	Использование контролируемого ИР (ОКИИ) для распространения ВПО (malware command and control), Компьютерная атака типа "отказ в обслуживании", направленная на контролируемый ИР (ОКИИ) (dos), Распределенная компьютерная атака типа "отказ в обслуживании", направленная на контролируемый ИР (ОКИИ) (ddos), Рассылка спам-сообщений с контролируемого ИР (ОКИИ) (spam)
Новое удаленное подключение к коммутатору Eltex по SSH	Попытки несанкционированного доступа в систему или к информации (intrusion attempt)	Попытки авторизации в контролируемом ИР (ОКИИ) (login attempt)
Сброс пароля пользователя	Нарушение безопасности информации (information content security)	Несанкционированное изменение информации, обрабатываемой в контролируемом ИР (ОКИИ) (unauthorised modification)
События IDS с высоким приоритетом	Сбор сведений с использованием ИКТ (information gathering)	Сканирование информационного ресурса (ОКИИ) (scanning)
Использование планировщика задач для ransomware	Заражение вредоносным программным обеспечением (malware)	Внедрение в контролируемый ИР (ОКИИ) модулей ВПО (malware infection)
SAM dump в AppData	Несанкционированный доступ в систему (intrusion)	Компрометация учетной записи в контролируемом ИР (ОКИИ) (account compromise)
Ошибка сбора данных с ОЗ	Нарушение или замедление работы контролируемого информационного ресурса (availability)	Непреднамеренное (без злого умысла) отключение ИР (ОКИИ) (outage), Несанкционированный вывод ИР (ОКИИ) из строя (sabotage)

Реагирование на инциденты

USSC

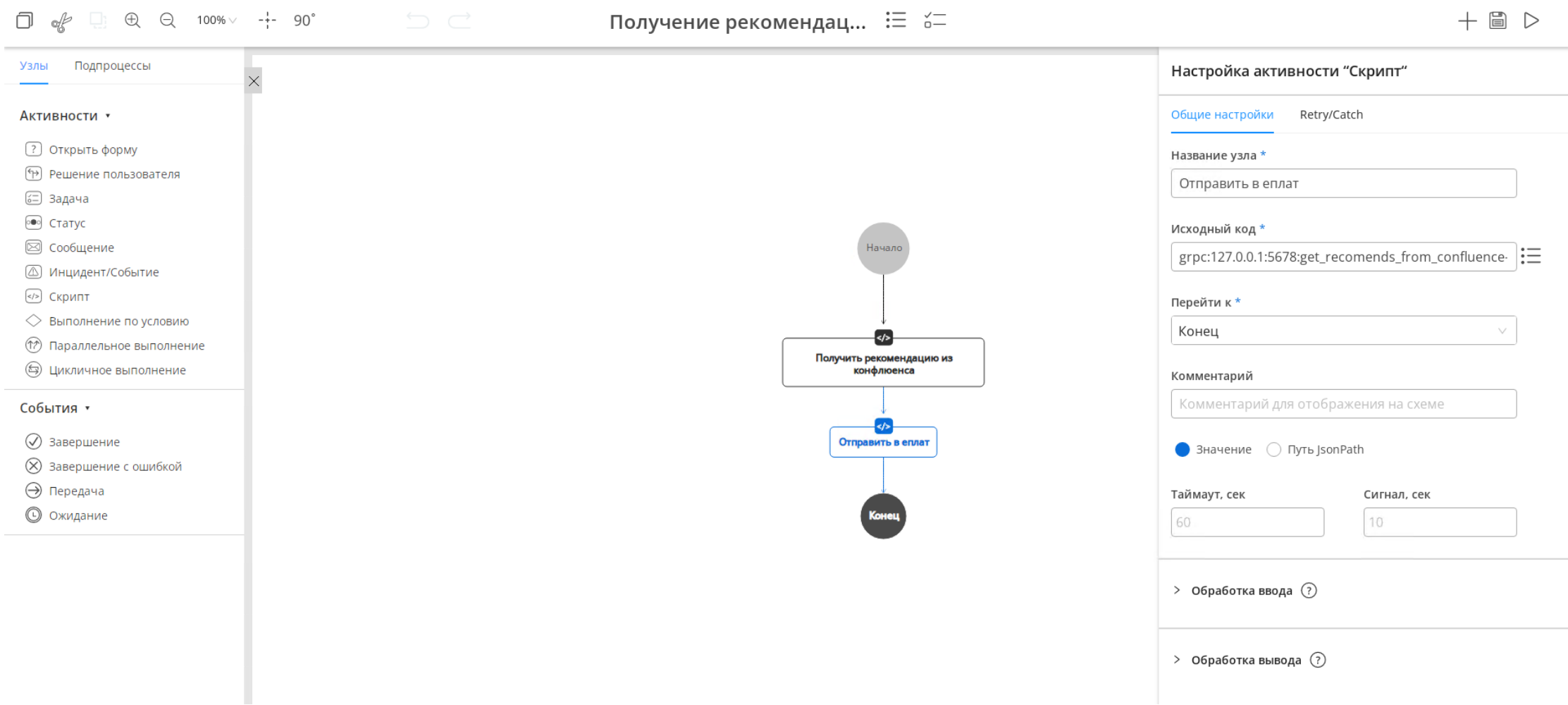
Функции:

- Создание и использование сценариев реагирования (плейбуков)
- Создание и использование скриптов автоматизации
- Управление расписанием
- Управление секретами
- Витрина плейбуков

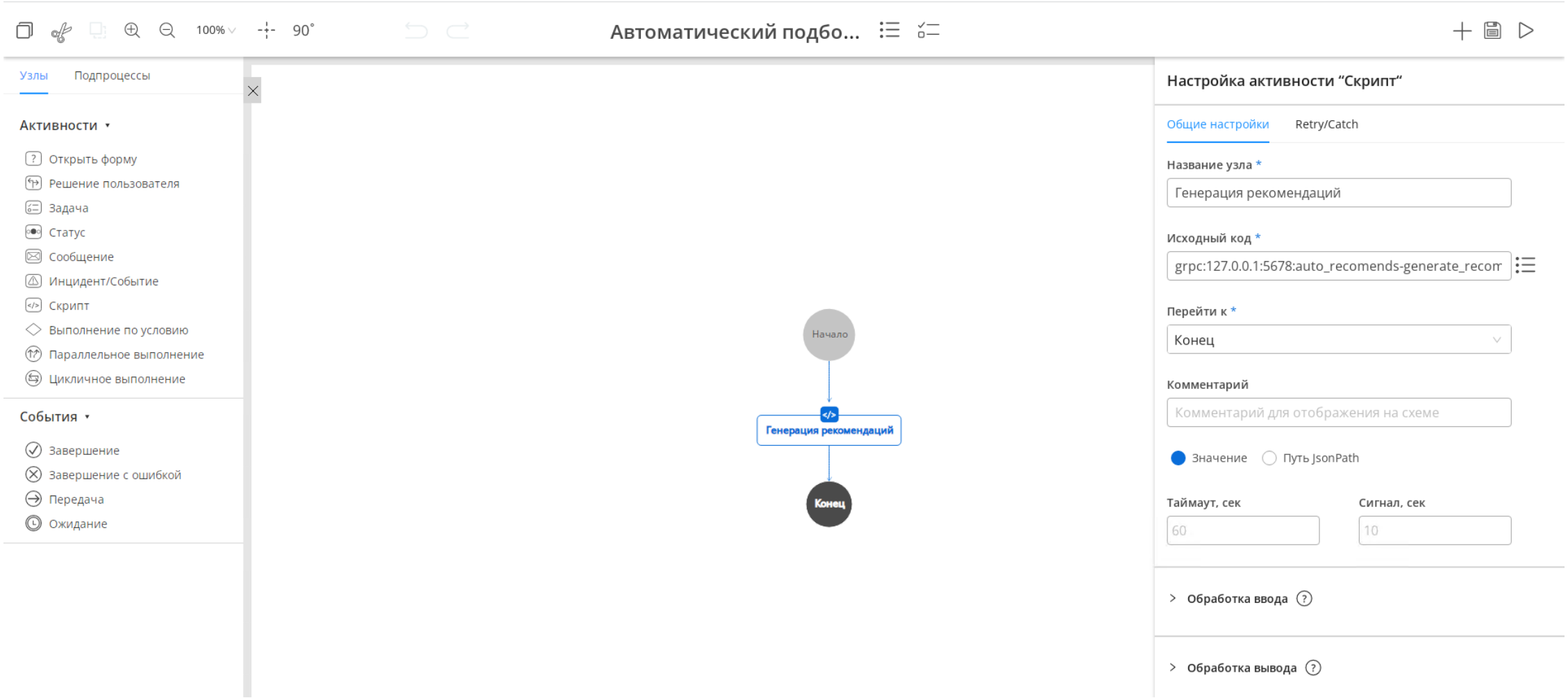
Реагирование осуществляется при помощи:

- Языка описания плейбуков Amazon States Language
- Скриптов на языках программирования Python, PowerShell, Bash

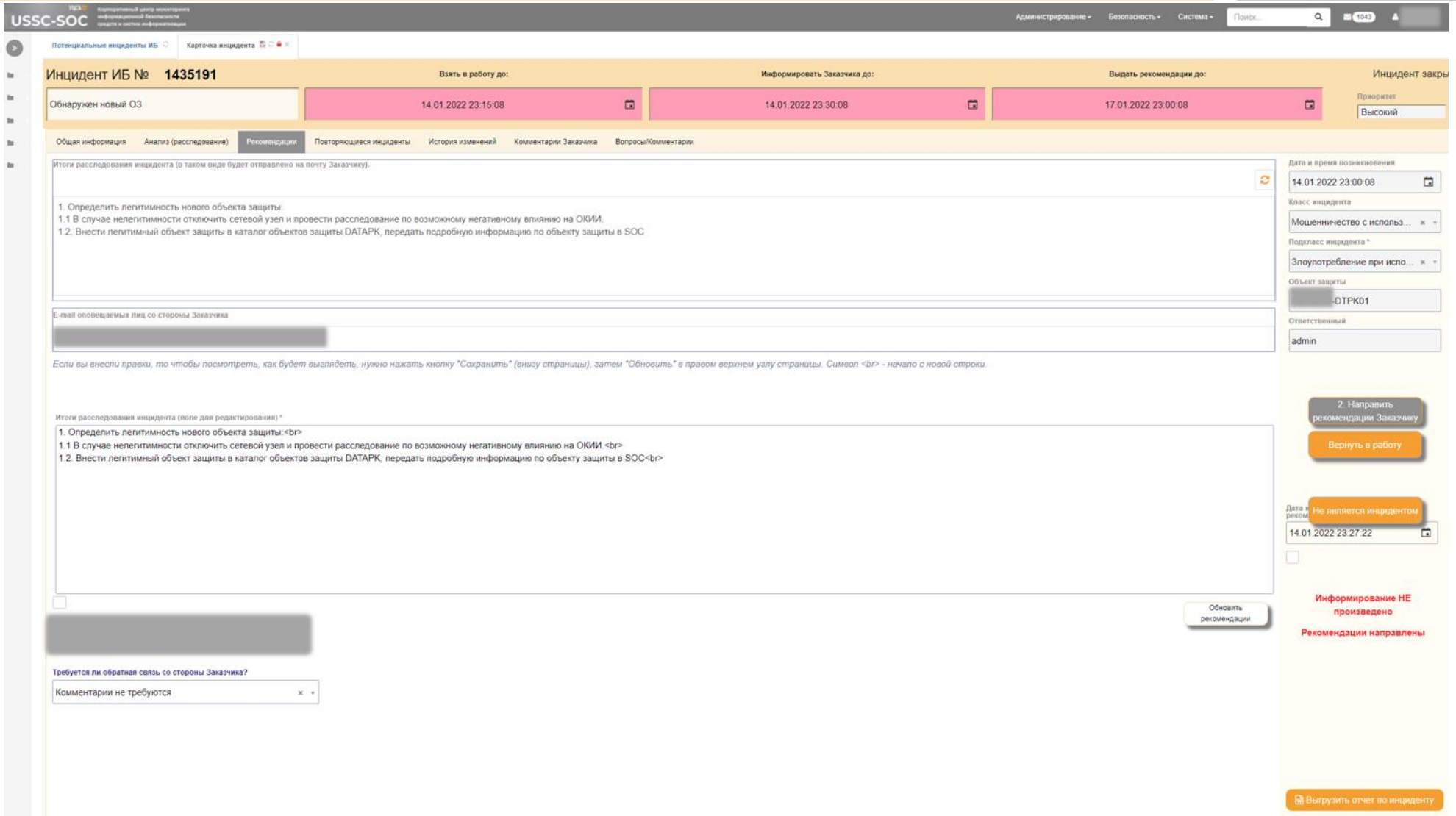
Пример плейбука реагирования



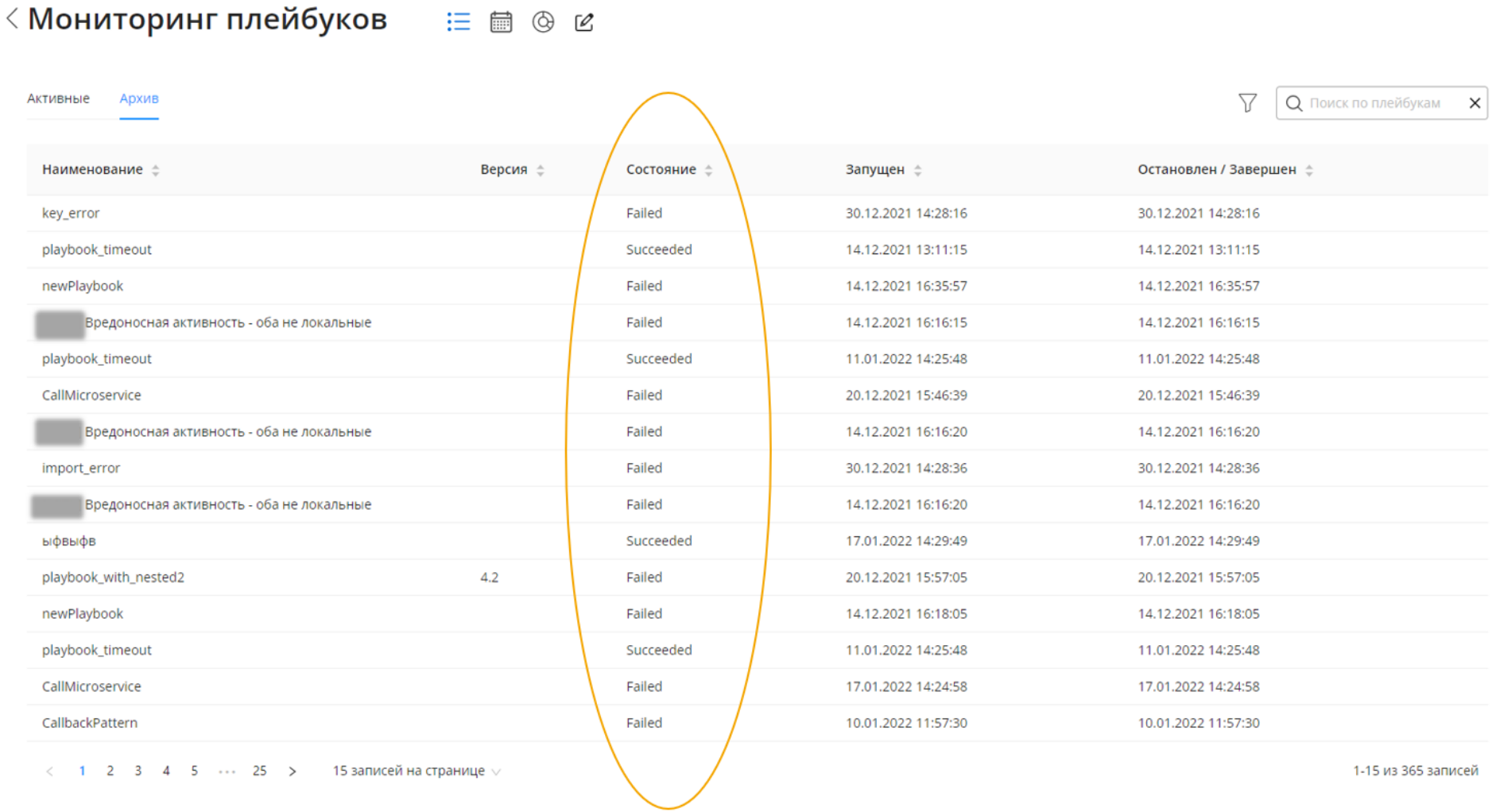
Пример выдачи рекомендаций по реагированию



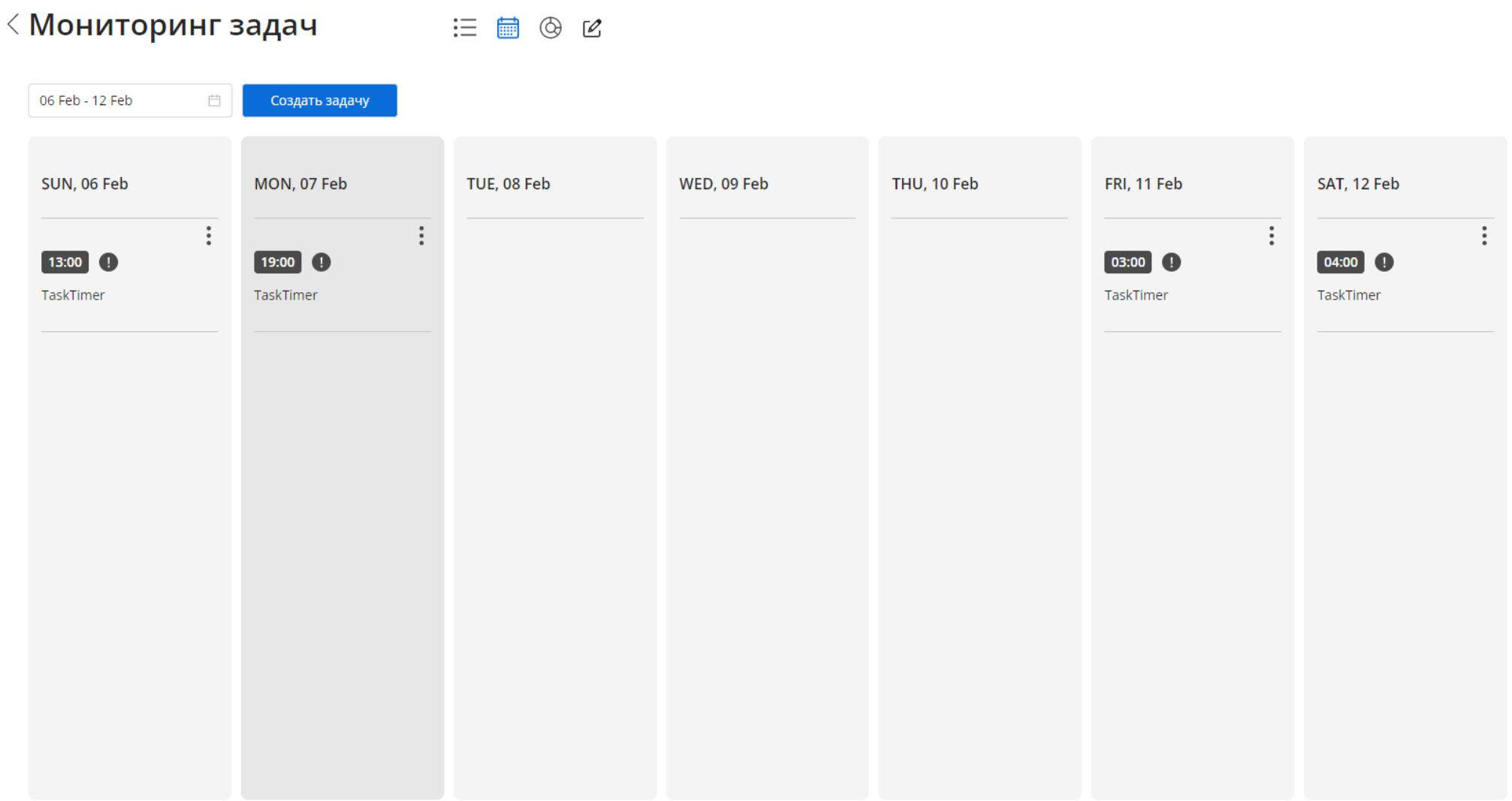
Рекомендации сформированы



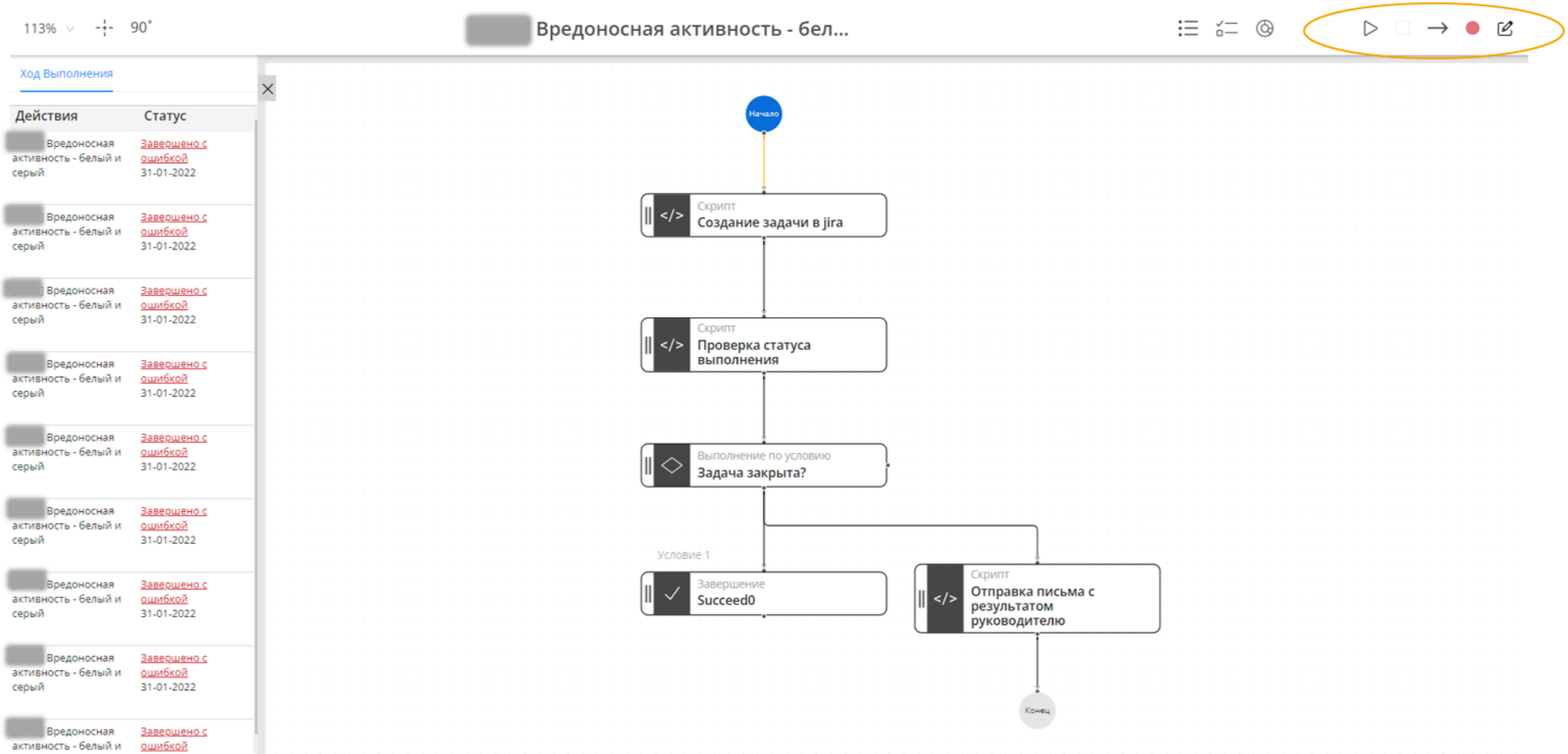
Мониторинг плейбуков



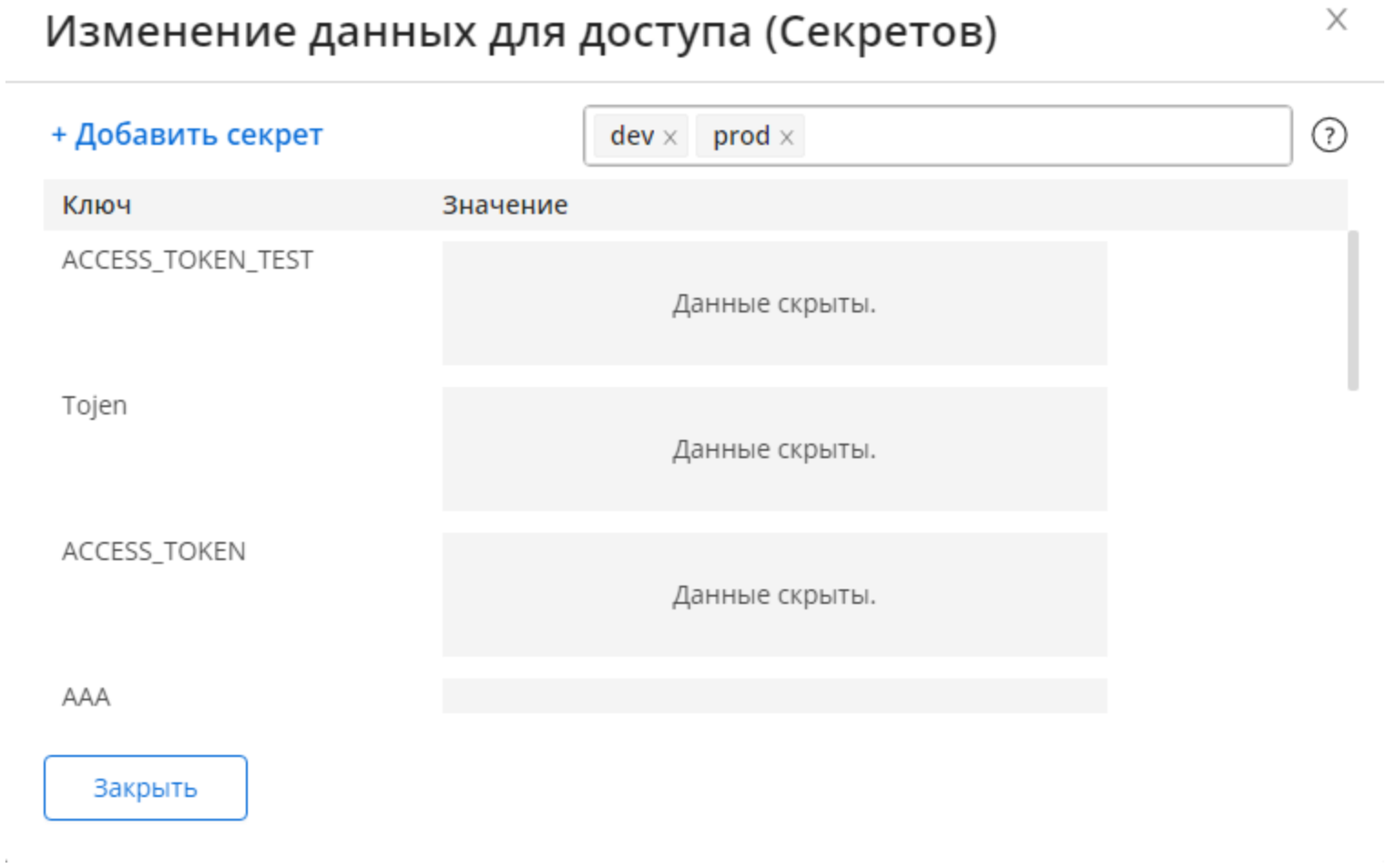
Планировщик плейбуков



Редактор и отладчик плейбуков



Модуль управления секретами



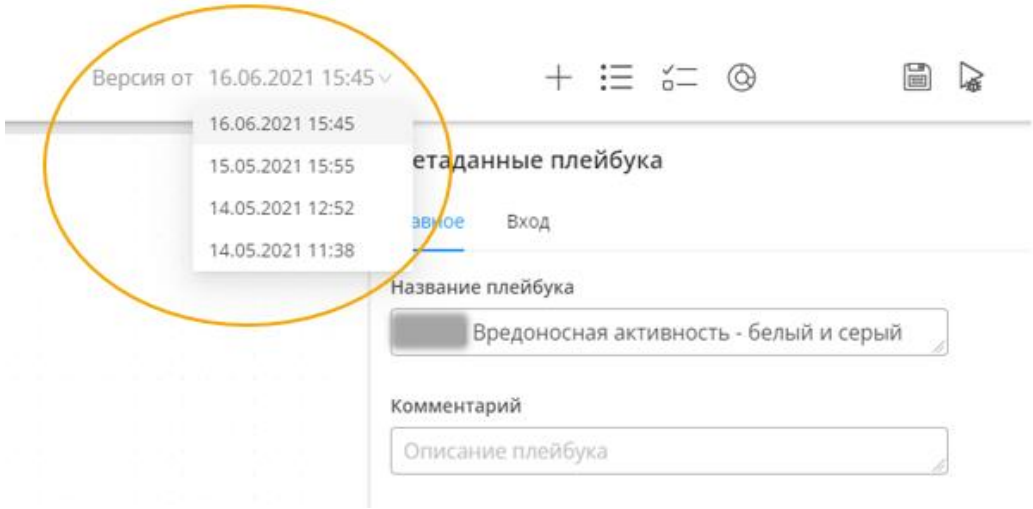
Иерархическая дистрибуция контента

USSC

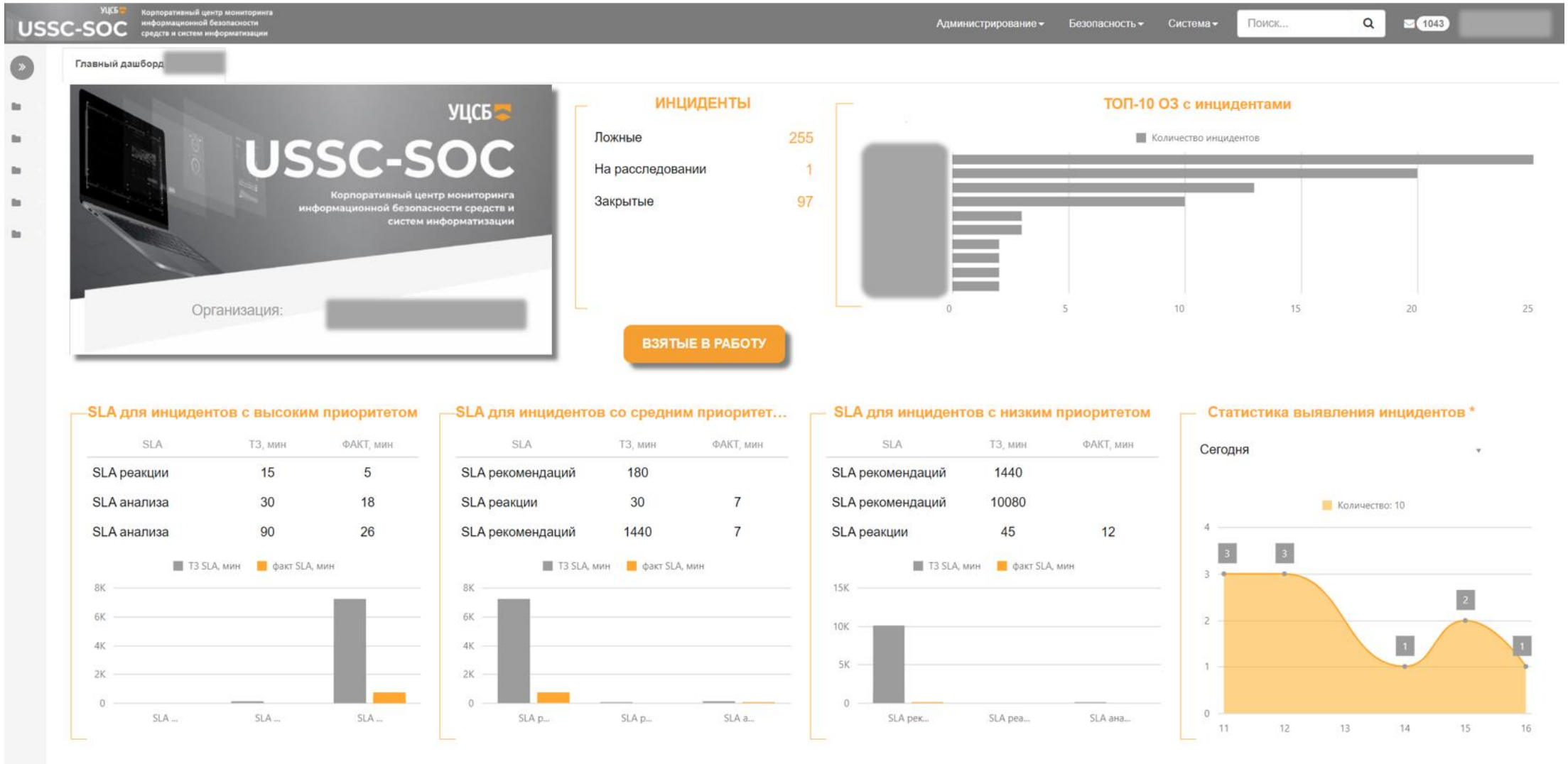
Централизованное версионированное хранилище

Обеспечивает единый механизм распространения сценариев обогащения, реагирования и восстановления для:

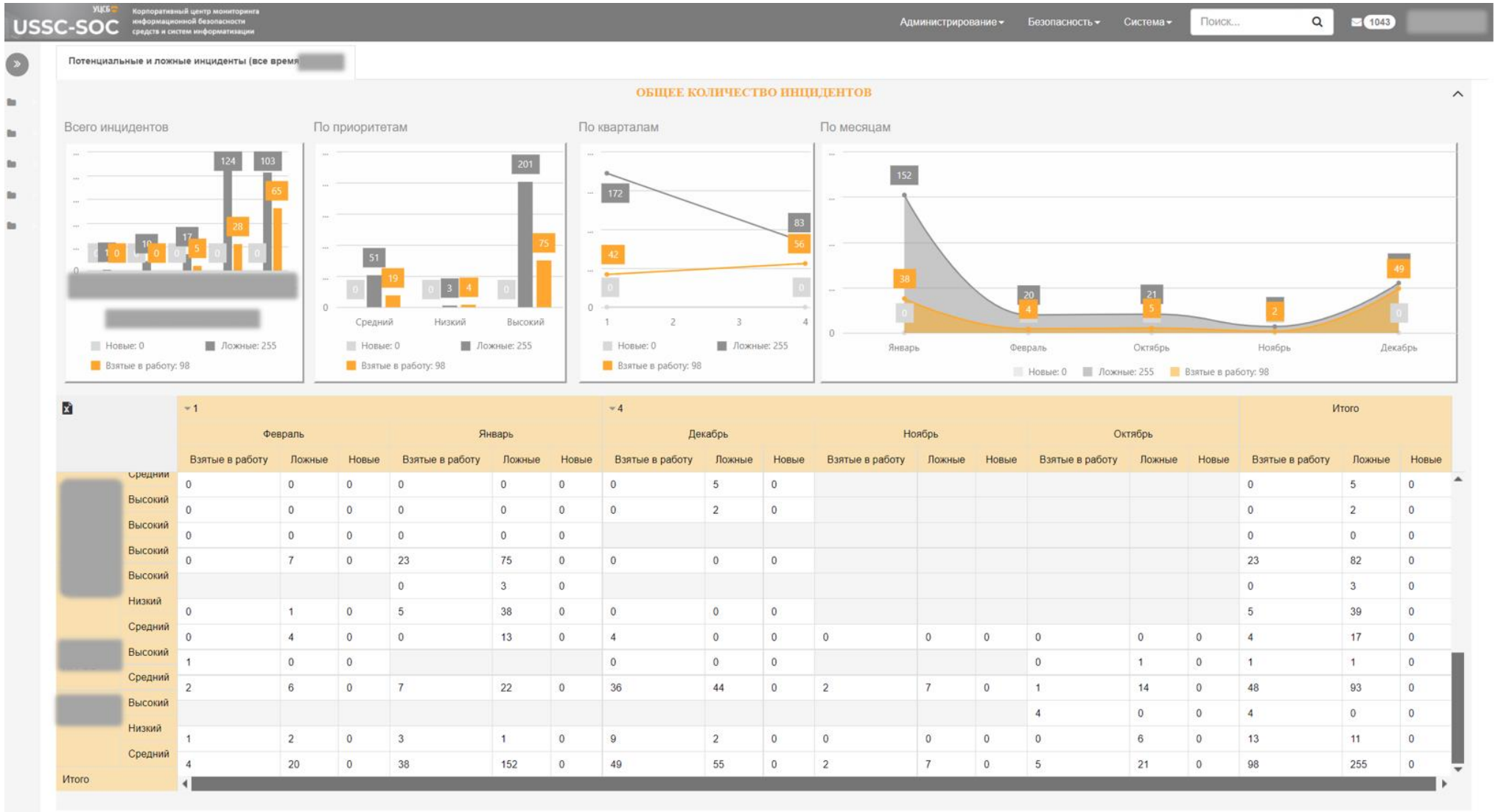
- Плейбуков
- Скриптов
- Секретов



Дашборд с общими показателями

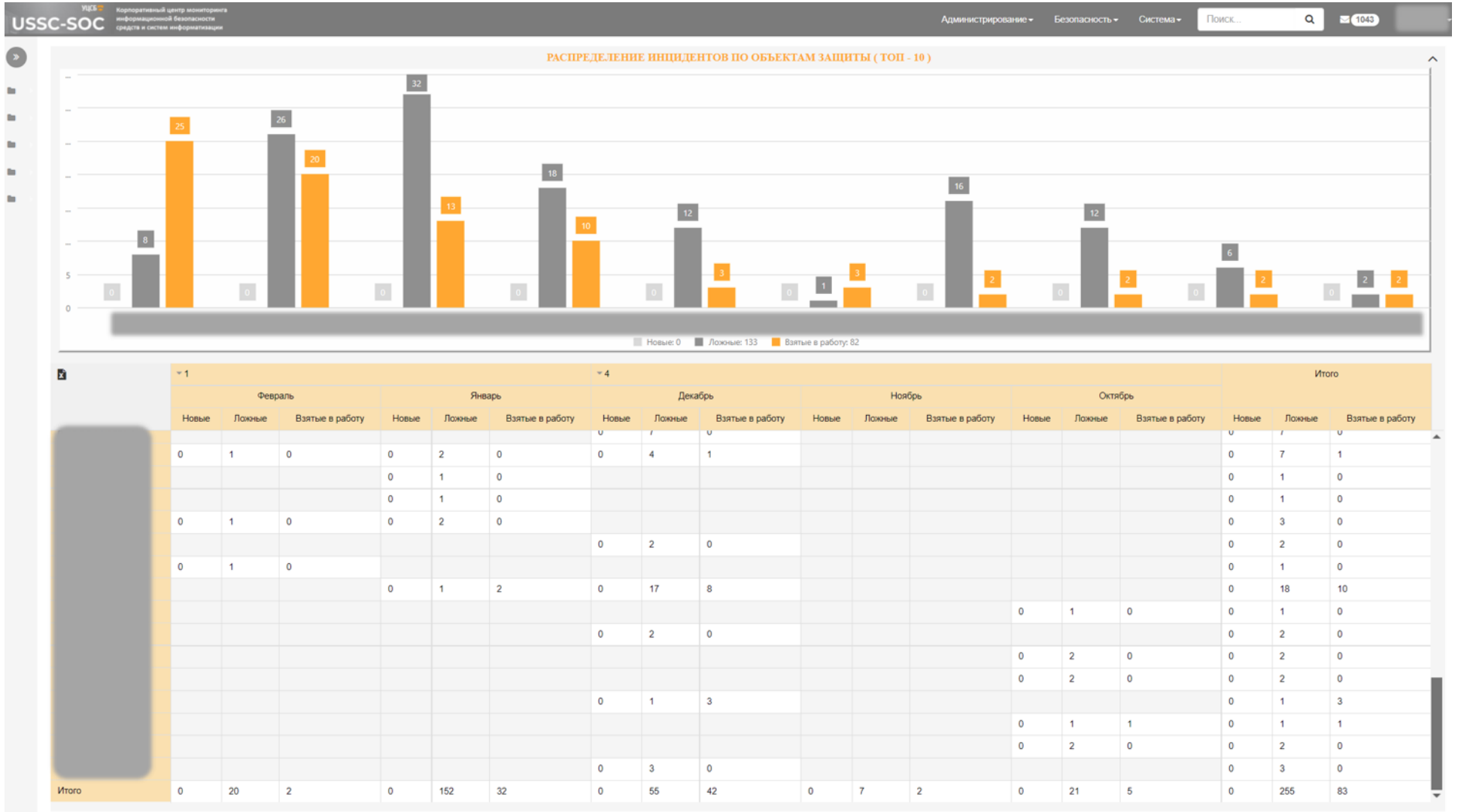


Отчетность по инцидентам



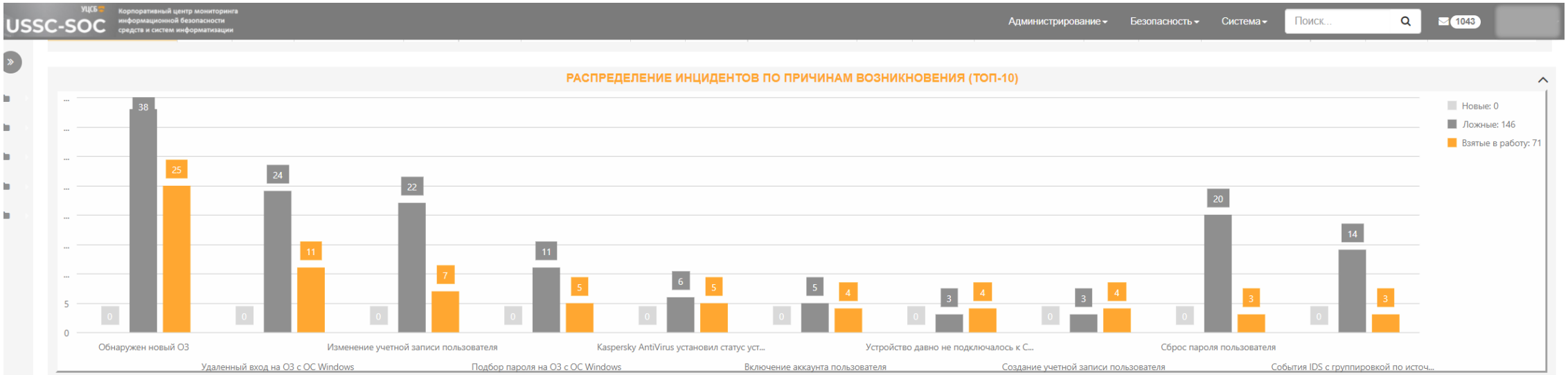
	1						4									Итого		
	Февраль			Январь			Декабрь			Ноябрь			Октябрь					
	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые
Средний	0	0	0	0	0	0	0	5	0							0	5	0
Высокий	0	0	0	0	0	0	0	2	0							0	2	0
Высокий	0	0	0	0	0	0										0	0	0
Высокий	0	7	0	23	75	0	0	0	0							23	82	0
Высокий				0	3	0										0	3	0
Низкий	0	1	0	5	38	0	0	0	0							5	39	0
Средний	0	4	0	0	13	0	4	0	0	0	0	0	0	0	0	4	17	0
Высокий	1	0	0				0	0	0				0	1	0	1	1	0
Средний	2	6	0	7	22	0	36	44	0	2	7	0	1	14	0	48	93	0
Высокий													4	0	0	4	0	0
Низкий	1	2	0	3	1	0	9	2	0	0	0	0	0	6	0	13	11	0
Средний	4	20	0	38	152	0	49	55	0	2	7	0	5	21	0	98	255	0
Итого																		

Отчетность по объектам защиты (активам)



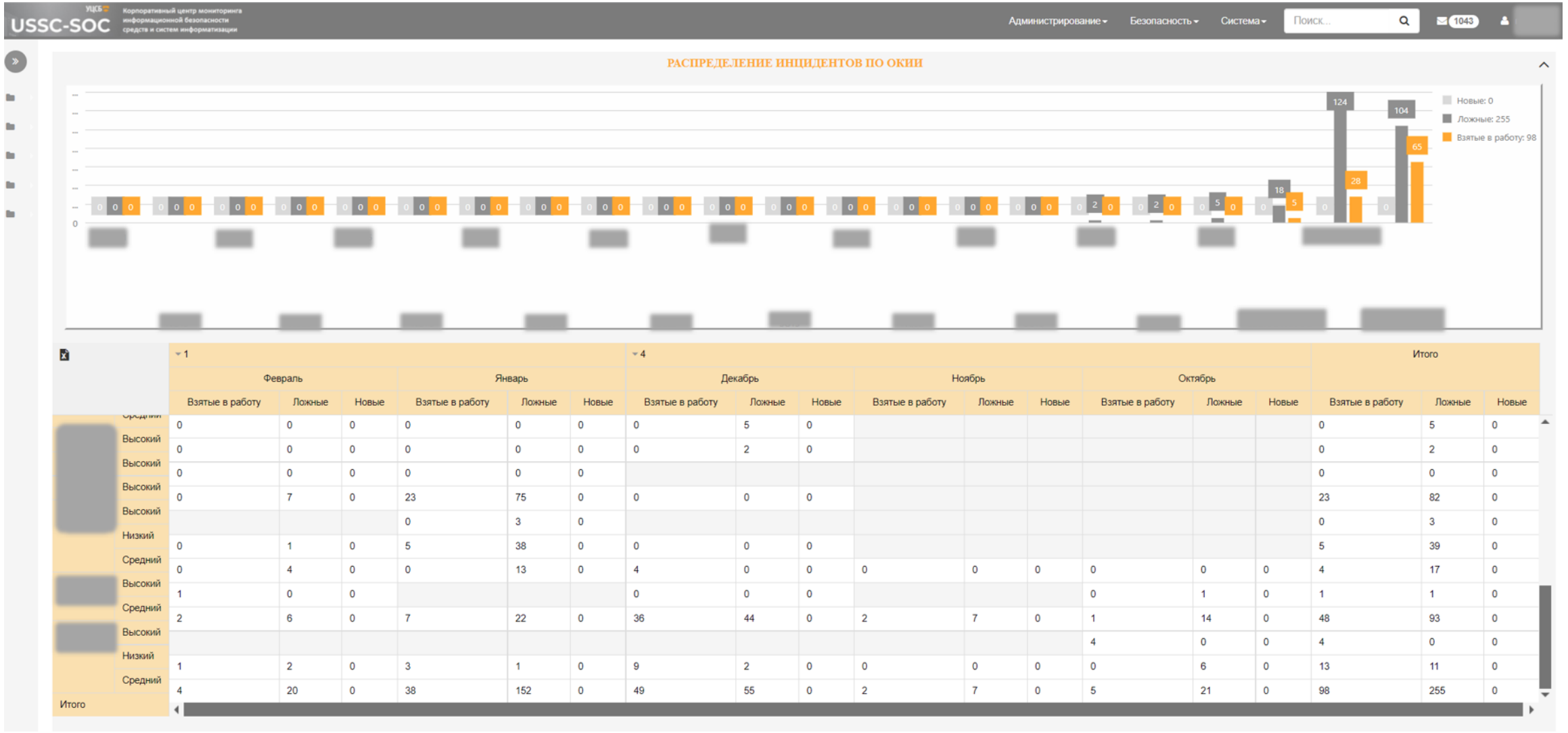
	1						4									Итого		
	Февраль			Январь			Декабрь			Ноябрь			Октябрь					
	Новые	Ложные	Взятые в работу	Новые	Ложные	Взятые в работу	Новые	Ложные	Взятые в работу	Новые	Ложные	Взятые в работу	Новые	Ложные	Взятые в работу	Новые	Ложные	Взятые в работу
							0	7	0							0	7	0
	0	1	0	0	2	0	0	4	1							0	7	1
				0	1	0										0	1	0
				0	1	0										0	1	0
	0	1	0	0	2	0										0	3	0
							0	2	0							0	2	0
	0	1	0													0	1	0
				0	1	2	0	17	8							0	18	10
													0	1	0	0	1	0
							0	2	0							0	2	0
													0	2	0	0	2	0
													0	2	0	0	2	0
							0	1	3							0	1	3
													0	1	1	0	1	1
													0	2	0	0	2	0
							0	3	0							0	3	0
Итого	0	20	2	0	152	32	0	55	42	0	7	2	0	21	5	0	255	83

Причины возникновения инцидентов



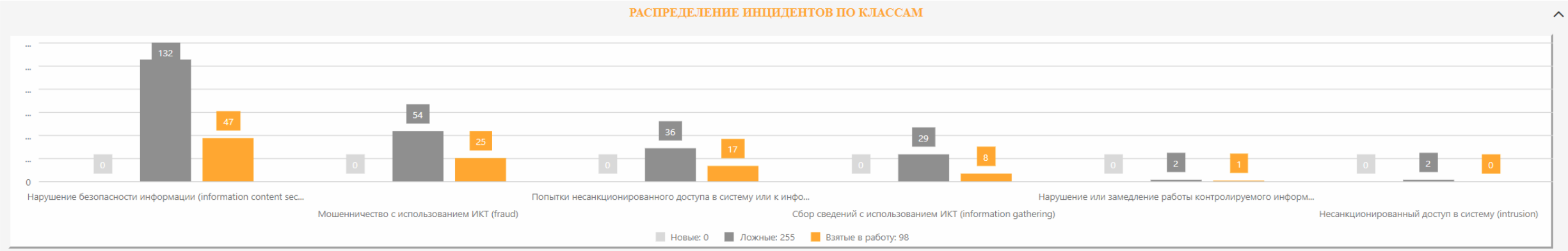
	1						4									Итого		
	Февраль			Январь			Декабрь			Ноябрь			Октябрь					
	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые
Kaspersky AntiVirus выключен	0	2	0				1	0	0							1	2	0
Kaspersky AntiVirus назначил управляемому устройству статус 'Критический' по неизвестной причине							0	1	0							0	1	0
Kaspersky AntiVirus назначил управляемому устройству статус 'Предупреждение' по неизвестной причине							0	4	0							0	4	0
Kaspersky AntiVirus обнаружил инцидент информационной безопасности							0	4	0							0	4	0
Kaspersky AntiVirus установил статус устройства 'критический'							5	6	0							5	6	0
Аккаунт пользователя был добавлен в глобальную группу	1	0	0	0	2	0	1	0	0							2	2	0
Аккаунт пользователя был добавлен в локальную группу	0	1	0	0	13	0	2	0	0				0	7	0	2	21	0
Аккаунт пользователя был удален из глобальной группы				0	1	0	0	1	0							0	2	0
Блокировка учетной записи							2	0	0							2	0	0
Включение аккаунта пользователя	0	1	0	0	3	0	4	1	0							4	5	0

Распределение инцидентов по ОКИИ



		1						4									Итого		
		Февраль			Январь			Декабрь			Ноябрь			Октябрь					
		Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые	Взятые в работу	Ложные	Новые
	Средний	0	0	0	0	0	0	0	5	0							0	5	0
	Высокий	0	0	0	0	0	0	0	2	0							0	2	0
	Высокий	0	0	0	0	0	0										0	0	0
	Высокий	0	7	0	23	75	0	0	0	0							23	82	0
	Высокий				0	3	0										0	3	0
	Низкий	0	1	0	5	38	0	0	0	0							5	39	0
	Средний	0	4	0	0	13	0	4	0	0	0	0	0	0	0	0	4	17	0
	Высокий	1	0	0				0	0	0				0	1	0	1	1	0
	Средний	2	6	0	7	22	0	36	44	0	2	7	0	1	14	0	48	93	0
	Высокий													4	0	0	4	0	0
	Низкий	1	2	0	3	1	0	9	2	0	0	0	0	0	6	0	13	11	0
	Средний	4	20	0	38	152	0	49	55	0	2	7	0	5	21	0	98	255	0
Итого																			

Распределение инцидентов по классам



	Необработанные	Ложные инциденты	Взятые в работу	Необработанные	Ложные инциденты	Взятые в работу	Необработанные	Ложные инциденты	Взятые в работу	Необработанные	Ложные инциденты	Взятые в работу	Необработанные	Ложные инциденты	Взятые в работу	Необработанные	Ложные инциденты	Взятые в работу
Мошенничество с использованием ИКТ (fraud)	0	1	1	0	45	22	0	8	2							0	54	25
Нарушение безопасности информации (information content security)	0	13	2	0	75	6	0	34	38				0	10	1	0	132	47
Нарушение или замедление работы контролируемого информационного ресурса (availability)	0	2	0				0	0	1							0	2	1
Несанкционированный доступ в систему (intrusion)				0	2	0										0	2	0
Попытки несанкционированного доступа в систему или к информации (intrusion attempt)	0	4	1	0	30	10	0	2	6							0	36	17
Сбор сведений с использованием ИКТ (information gathering)	0	0	0	0	0	0	0	11	2	0	7	2	0	11	4	0	29	8
Итого	0	20	4	0	152	38	0	55	49	0	7	2	0	21	5	0	255	98

Результаты внедрения SOAR

Уменьшение числа обрабатываемых вручную инцидентов

Снижение времени реагирования

Автоматизация обогащения и агрегации инцидентов

USSC

СПАСИБО ЗА ВНИМАНИЕ

ВОПРОСЫ?

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU