



CNews FORUM Кейсы Опыт ИТ-лидеров

**ПРОЦЕСС УПРАВЛЕНИЯ
УЯЗВИМОСТЯМИ:
ОПЫТ ИМПОРТОЗАМЕЩЕНИЯ**

**ОЛЕГ КУСЕРОВ,
ДИРЕКТОР ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НРД**



КТО МЫ?

МОЕХ GROUP ФИН УСЛУГИ

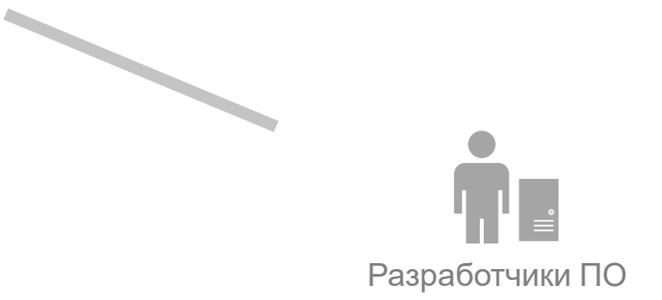
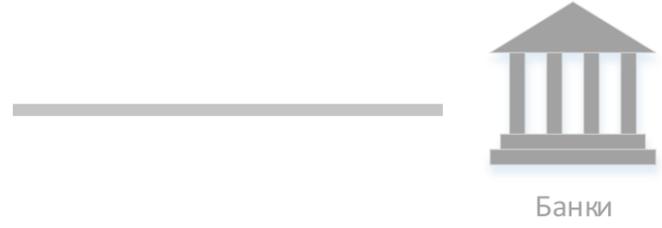


НТБ
Товарная биржа

Московская Биржа
Фондовый рынок
Валютный рынок
Денежный рынок
Срочный рынок

НКЦ
Клиринговый центр
Центральный контрагент на всех рынках

НРД
Центральный депозитарий
Расчетный центр
Регистратор финансовых транзакций



ИТ инфраструктура, телекоммуникации, разработка ПО

ПРОЦЕСС УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ ДО 2022 ГОДА



КЛЮЧЕВЫЕ ПРОБЛЕМЫ ПРИ ИМЕЮЩЕМСЯ ПОДХОДЕ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

01

ОТСУТСТВИЕ
ПОНИМАНИЯ ГРАНИЦ
ЗАЩИЩАЕМЫХ ОБЪЕКТОВ

02

ДЛИТЕЛЬНОЕ ВРЕМЯ
ОБРАБОТКИ ОБНАРУЖЕННЫХ
УЯЗВИМОСТЕЙ

03

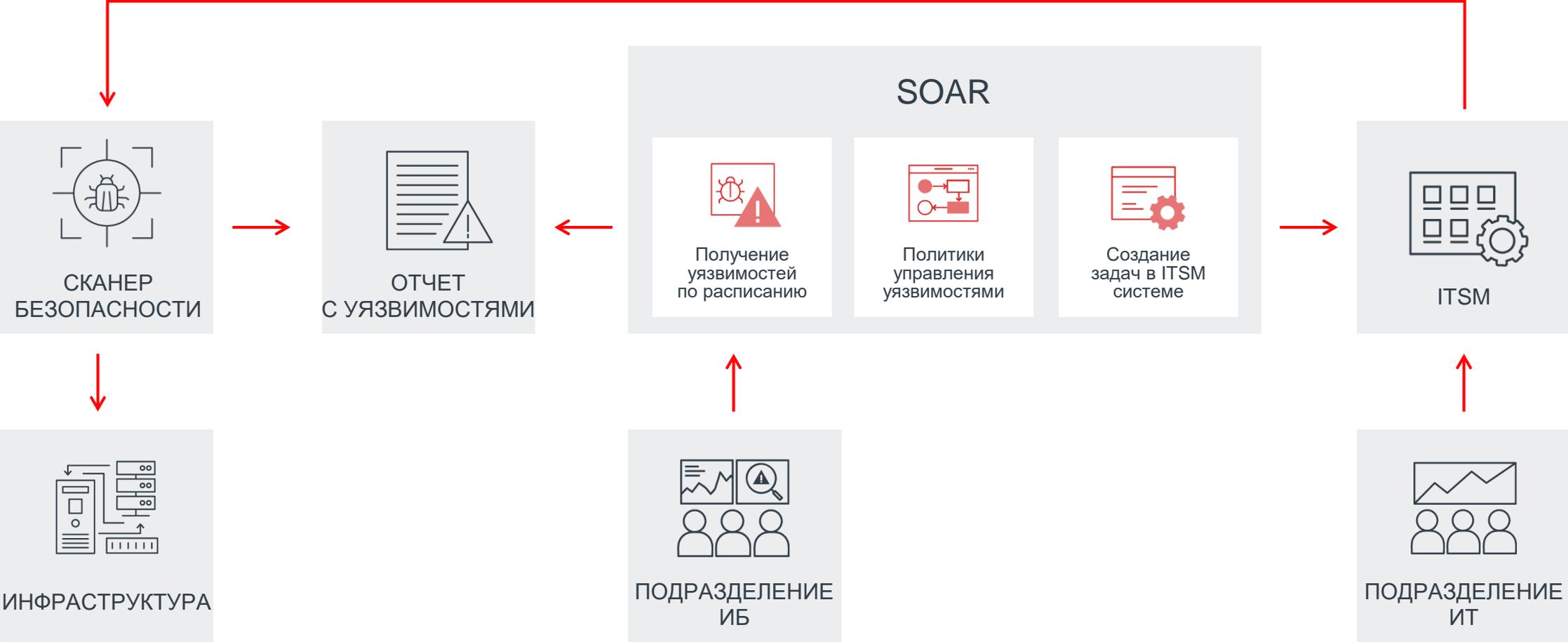
БЕССИСТЕМНОЕ
УСТРАНЕНИЕ
УЯЗВИМОСТЕЙ

04

ОТСУТСТВИЕ ПОЛНОГО
КОНТРОЛЯ УСТРАНЕНИЯ
УЯЗВИМОСТЕЙ



ПРОЦЕСС УПРАВЛЕНИЯ УЯЗВИМОСТЕЙ ПОСЛЕ ВНЕДРЕНИЯ SOAR



ФОРМУЛА РАСЧЕТА РЕЙТИНГА

Расчет рейтинга уязвимости

Статус: Посчитать сейчас Отмена Сохранить

Формула расчета рейтинга уязвимости
 $(CVSS+DEVCR*2+ASSETCR*2)*VULSTATUS/3$

① Рейтинг уязвимости рассчитывается для каждой уязвимости на хосте. Рейтинг уязвимости рассчитывается на основе оценки **CVSS**, поэтому эту переменную нельзя удалить. Система работает с двумя версиями оценки **CVSS: V2** и **V3**. По умолчанию используется **CVSS V3**, если для уязвимости доступны обе оценки. В остальных случаях используется **CVSS V2**. Для расчета рейтинга могут использоваться поля **Уязвимости** и поля с типом **Справочник** или **Чек-бокс** активов **Оборудование**, **Группы ИТ-активов**. После добавления в формулу каждому значению поля нужно задать коэффициент, который будет заменять текстовое значение поля при расчете.

Переменные

Добавить	Удалить	Поле актива
ID		
CVSS		
DEVCR		
ASSETCR		
VULSTATUS		

Формула расчета рейтинга уязвимости
 $(CVSS+DEVCR*2+ASSETCR*2)*VULSTATUS/3$

Список значений :

Значение	Коэффициент
----------	-------------



**Стабильная работа в сделку не
входила**

РЕКОМЕНДАЦИИ

РЕКОМЕНДАЦИИ НКЦКИ ОТ 15 АПРЕЛЯ 2022 ГОДА



РЕКОМЕНДАЦИИ ФСТЭК ОТ 17 МАЯ 2023 ГОДА



МОДЕРНИЗАЦИЯ ПРОЦЕССА

3 ГЛАВНЫХ СПРИНТА

01

ПЕРЕХОД НА НОВЫЙ
ОТЕЧЕСТВЕННЫЙ
СКАНЕР

02

ПЕРЕХОД НА НОВУЮ
ОТЕЧЕСТВЕННУЮ
ITSM

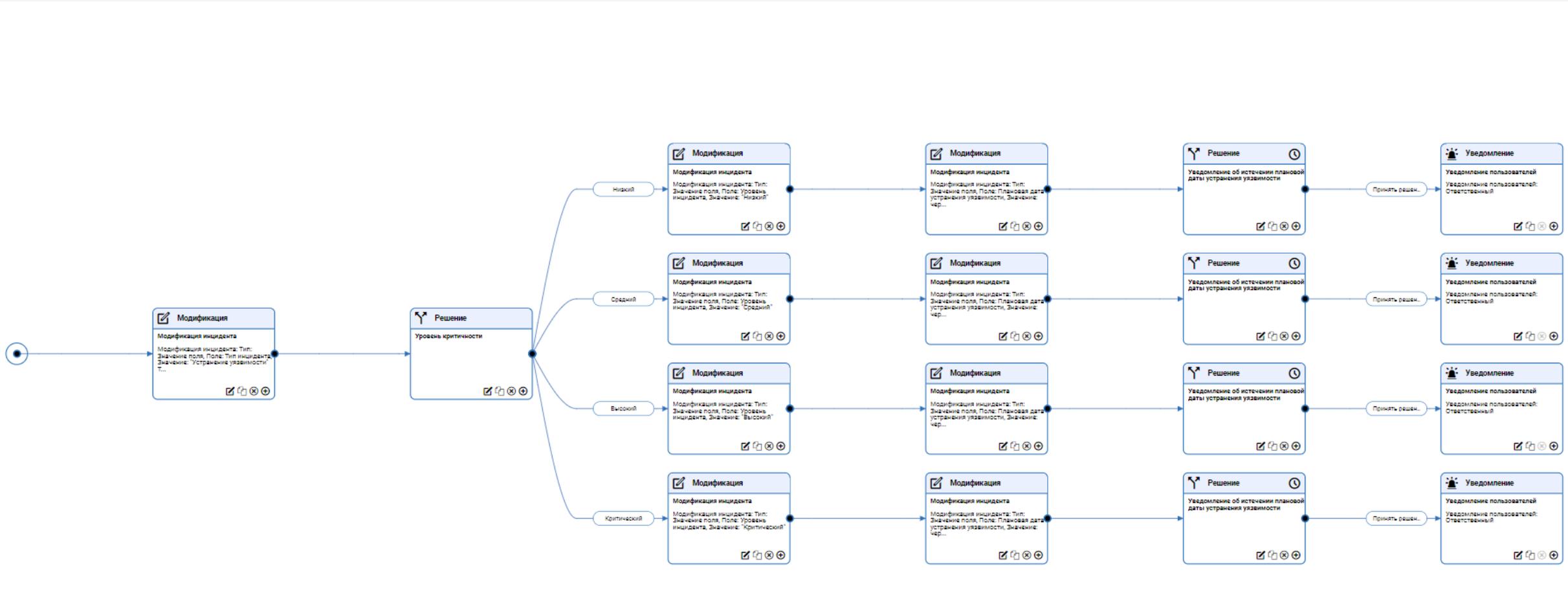
03

АДАПТАЦИЯ ПРОЦЕССА
С УЧЕТОМ
РЕКОМЕНДАЦИЙ
ОТ НКЦКИ, ФСТЭК

ПРОЦЕСС УПРАВЛЕНИЯ УЯЗВИМОСТЕЙ ПОСЛЕ 2022 ГОДА



SERVICE LEVEL AGREEMENT



SERVICE LEVEL AGREEMENT

Инциденты

Уязвимость ×

ID	Дата создания	Название уязвимости	Статус ...	Уровень ...	Рейтинг...	Оценка CVSS v.2	Оценка CVSS v.3	Вектор v2	Вектор v3	Просрочено время находж...	Просрочено в
23-04-84	26.04.2023 13:33:43		Назначен		4.8	3	7	AV:N/AC:L/Au:S/C:C/I:C/A:C	AV:N/AC:L/Au:S/C:C/I:C/A:C		
23-04-83	26.04.2023 13:26:54		Назначен								
23-04-82	26.04.2023 13:22:02		Назначен								
23-04-81	26.04.2023 13:21:39		Назначен								
23-04-76	23.04.2023 22:28:08		Новый								
23-04-74	23.04.2023 22:25:38		В работе								
23-04-73	23.04.2023 22:15:33		Выполн...								
23-04-72	23.04.2023 22:12:21		Новый								
23-04-71	23.04.2023 22:07:40		Новый								
23-04-70	23.04.2023 21:57:12		Назначен								
23-04-69	23.04.2023 18:42:50		В работе								
23-04-68	23.04.2023 18:40:40		В работе								
23-04-67	23.04.2023 18:37:49		Новый								
23-04-66	23.04.2023		Новый								

SLA

Полное время работы над инцидентом:
154 д 18:07:47

Время взятия в работу (приостановлено):
01:52:18

Просрочено время взятия в работу

Время устранения уязвимости:
154 д 16:15:29

Просрочено время устранения уязвимости

Время нахождения ЗНУ в ожидании (приостановлено):
00:07:42

Просрочено время нахождения ЗНУ в ожидании

Плановая дата устранения уязвимости [UTC+03:00]
30.09.2023

18:42:55

SLA

Полное время работы над инцидентом:
154 д 18:07:47

Время взятия в работу (приостановлено):
01:52:18

Просрочено время взятия в работу

Время устранения уязвимости:
154 д 16:15:29

Просрочено время устранения уязвимости

Время нахождения ЗНУ в ожидании (приостановлено):
00:07:42

Просрочено время нахождения ЗНУ в ожидании

Плановая дата устранения уязвимости [UTC+03:00]
30.09.2023

18:42:55

Страница 1 из 3 50 Поиск...

Отображаются записи с 1 по 50, всего 143

КРИТЕРИИ, ПРЕДЪЯВЛЯЕМЫЕ К СКАНЕРАМ БЕЗОПАСНОСТИ

01

СКАНИРОВАНИЕ UNIX,
WIN И IBM-СЕРВЕРА

02

СКАНИРОВАНИЕ
АКТИВНОГО СЕТЕВОГО
ОБОРУДОВАНИЯ

03

КОНТРОЛЬ
КОНФИГУРАЦИЙ

ПРЕИМУЩЕСТВА VM

01

АВТОПОДБОР
УЧЕТНЫХ
ЗАПИСЕЙ

02

ВЫСОКАЯ
СКОРОСТЬ
СКАНИРОВАНИЯ

03

ОБОРУДОВАНИЕ
ПОЯВЛЯЕТСЯ СРАЗУ
ПО ХОДУ
СКАНИРОВАНИЯ

04

ШИРОКИЕ
ВОЗМОЖНОСТИ
ИНТЕГРАЦИИ



СПАСИБО
ЗА ВНИМАНИЕ