

SPACE·BIT

 **SpaceView**

**Система мониторинга и
реагирования на инциденты
информационной безопасности**

www.spacebit.ru



Реальность 2023 – угрозы ИБ изменились

2022 – год **беспрецедентного роста ИБ угроз**. Угрозы изменились качественно и количественно (vs 2021) и тенденция сохраняется.

+700% кол-во DDOS атак * **+300%** выросло кол-во инцидентов ИБ *

20% атак трудно расследовать специалистам по ИБ без специальных средств *



новые виды угроз: через open source решения, мессенджеры, закрытые каналы Telegram, сильно модифицировались методы фишинга *



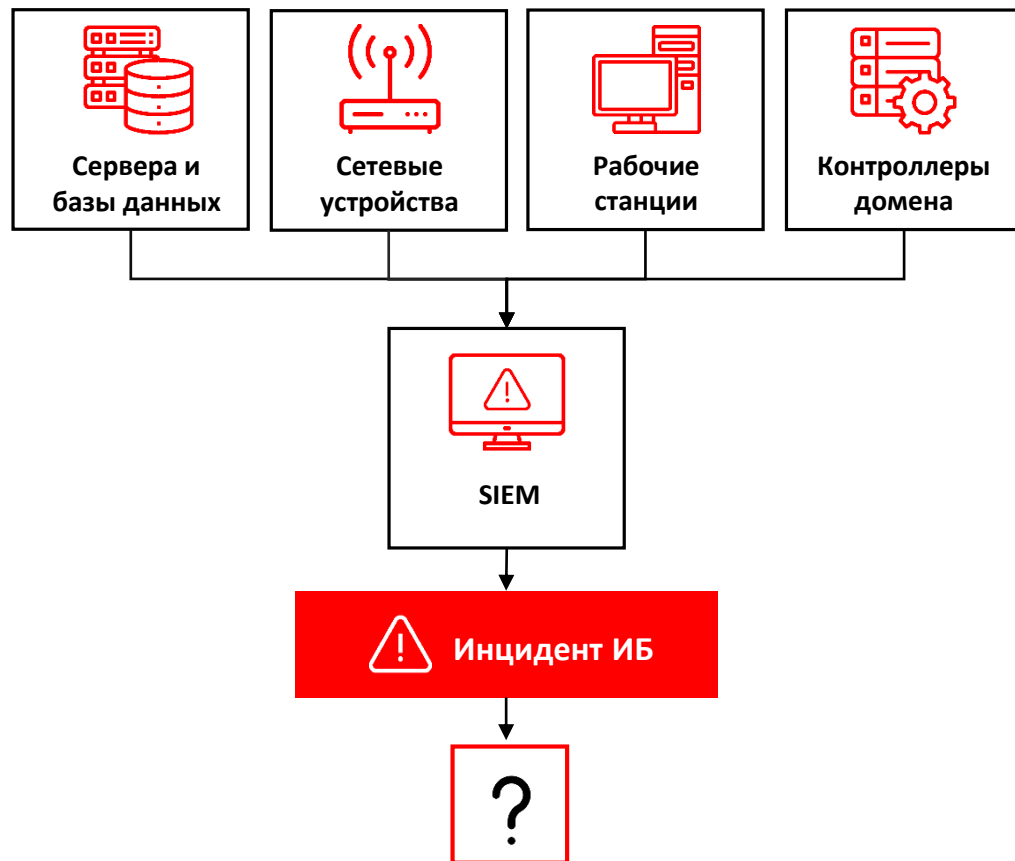
активным атакам подвергся даже SMB сектор, атакуемый ранее крайне редко*



*По данным тематических обзоров экспертов Positive Technologies, Лаборатории Касперского, КРОК

Реальность 2023 – как обеспечить безопасность

Имеющиеся средства обеспечения ИБ (SIEM, EDR, XDR, Service Desk, и др.) не всегда могут обеспечивать решение ключевых задач, стоящих перед сотрудниками службы ИБ.



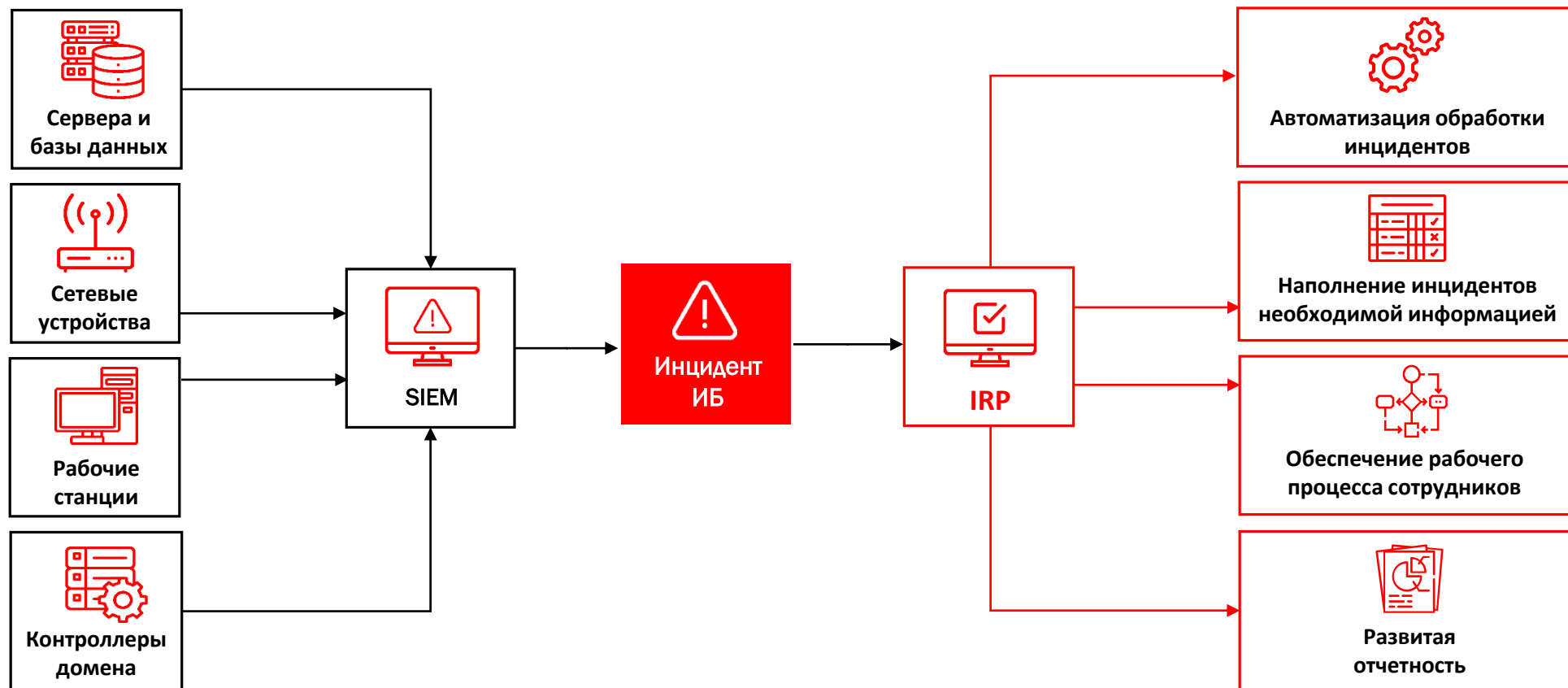
Основные проблемы, с которыми часто сталкиваются сотрудники службы ИБ:

- **Отсутствие единой системы** консолидации данных об инцидентах и активах
- **Низкая скорость реакции** на инциденты, потеря времени при расследовании инцидентов
- Высокий процент **пропущенных инцидентов**
- **Отсутствие статистики** и средств аналитики

Что такое **IRP**?

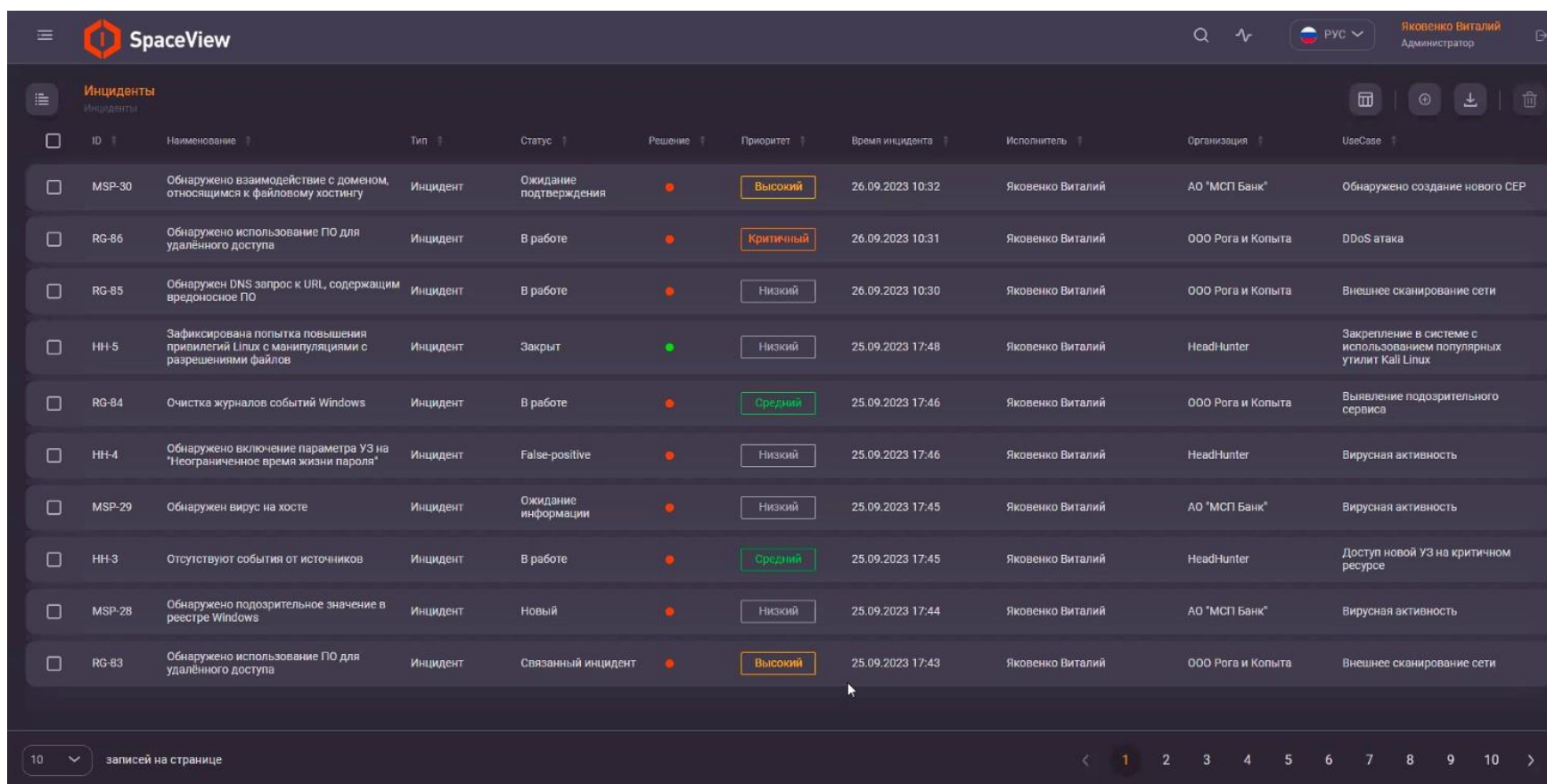
IRP (Incident Response Platform) — платформа для автоматизации реагирования на инциденты ИБ.

Системы класса IRP помогают сотрудникам ИБ сэкономить время и ресурсы при столкновении с кибератаками, а также повысить эффективность сдерживания, расследования и ликвидации последствий инцидентов.



Что такое SpaceView?

SpaceView - система класса IRP, предназначенная для мониторинга и оперативного реагирования на инциденты ИБ. Это единый центр управления, в котором агрегируются инциденты из различных источников.



The screenshot displays the SpaceView web interface. At the top, there is a navigation bar with the SpaceView logo, a search icon, a language dropdown set to 'РУС', and the user profile 'Яковенко Виталий, Администратор'. Below the navigation bar, the main content area is titled 'Инциденты' (Incidents). A table lists various security incidents with columns for ID, Name, Type, Status, Solution, Priority, Time, Executor, Organization, and UseCase. The incidents are sorted by time, with the most recent at the top. The priority levels are color-coded: High (yellow), Critical (orange), Low (grey), and Medium (green).

ID	Наименование	Тип	Статус	Решение	Приоритет	Время инцидента	Исполнитель	Организация	UseCase
MSP-30	Обнаружено взаимодействие с доменом, относящимся к файловому хостингу	Инцидент	Ожидание подтверждения		Высокий	26.09.2023 10:32	Яковенко Виталий	АО "МСП Банк"	Обнаружено создание нового СЕР
RG-86	Обнаружено использование ПО для удалённого доступа	Инцидент	В работе		Критичный	26.09.2023 10:31	Яковенко Виталий	ООО Рога и Копыта	DDoS атака
RG-85	Обнаружен DNS запрос к URL, содержащим вредоносное ПО	Инцидент	В работе		Низкий	26.09.2023 10:30	Яковенко Виталий	ООО Рога и Копыта	Внешнее сканирование сети
NN-5	Зафиксирована попытка повышения привилегий Linux с манипуляциями с разрешениями файлов	Инцидент	Закрыт		Низкий	25.09.2023 17:48	Яковенко Виталий	HeadHunter	Закрепление в системе с использованием популярных утилит Kali Linux
RG-84	Очистка журналов событий Windows	Инцидент	В работе		Средний	25.09.2023 17:46	Яковенко Виталий	ООО Рога и Копыта	Выявление подозрительного сервиса
NN-4	Обнаружено включение параметра УЗ на "Неограниченное время жизни пароля"	Инцидент	False-positive		Низкий	25.09.2023 17:46	Яковенко Виталий	HeadHunter	Вирусная активность
MSP-29	Обнаружен вирус на хосте	Инцидент	Ожидание информации		Низкий	25.09.2023 17:45	Яковенко Виталий	АО "МСП Банк"	Вирусная активность
NN-3	Отсутствуют события от источников	Инцидент	В работе		Средний	25.09.2023 17:45	Яковенко Виталий	HeadHunter	Доступ новой УЗ на критичном ресурсе
MSP-28	Обнаружено подозрительное значение в реестре Windows	Инцидент	Новый		Низкий	25.09.2023 17:44	Яковенко Виталий	АО "МСП Банк"	Вирусная активность
RG-83	Обнаружено использование ПО для удалённого доступа	Инцидент	Связанный инцидент		Высокий	25.09.2023 17:43	Яковенко Виталий	ООО Рога и Копыта	Внешнее сканирование сети

At the bottom of the table, there is a pagination control showing '10 записей на странице' and a set of page numbers from 1 to 10.

Какие задачи решает SpaceView



Автоматизация реагирования

Единый механизм реагирования на инциденты, возникающие в ходе эксплуатации ИТ-инфраструктуры, своевременное отслеживание их статуса и степени критичности



Оповещение об инцидентах

Автоматическое оперативное оповещение ответственных сотрудников об угрозах ИБ через популярные каналы связи (почта, мессенджеры и др.)



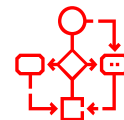
Визуализация данных и аналитика

Формирование информативных статистических отчетов для оценки текущих угроз ИБ и планирования дальнейших защитных и профилактических мероприятий



Агрегация данных об инцидентах

Объединение информации об угрозах из разных источников, ведение и учет карточек инцидентов, регистрация действий пользователей при обработке инцидентов



Поддержка рабочих процессов

Обеспечение совместной работы команд реагирования: выстраивание workflow, распределение задач между ИБ-специалистами, обмен данными между всеми участниками процесса



Помощь в расследовании инцидентов

Удобные поиск, фильтрация и группировка инцидентов по заданным критериям для более пристального изучения деталей отдельных инцидентов или групп инцидентов

Кому подойдет SpaceView?



В компании **есть SIEM**, но обработка инцидентов выполняется в ручном режиме



Ваша цель – **рациональное использование ИБ-бюджета** с максимальной эффективностью, сокращение трудозатрат



В компании есть сформированные правила и политики реагирования на инциденты ИБ и **требуется автоматизация процессов**

Почему SpaceView?



Гибкое ценообразование



Быстрое внедрение



Востребованный функционал



Возможность кастомизации



Удобный интерфейс



Собственный SOC ГК «Информзащита»

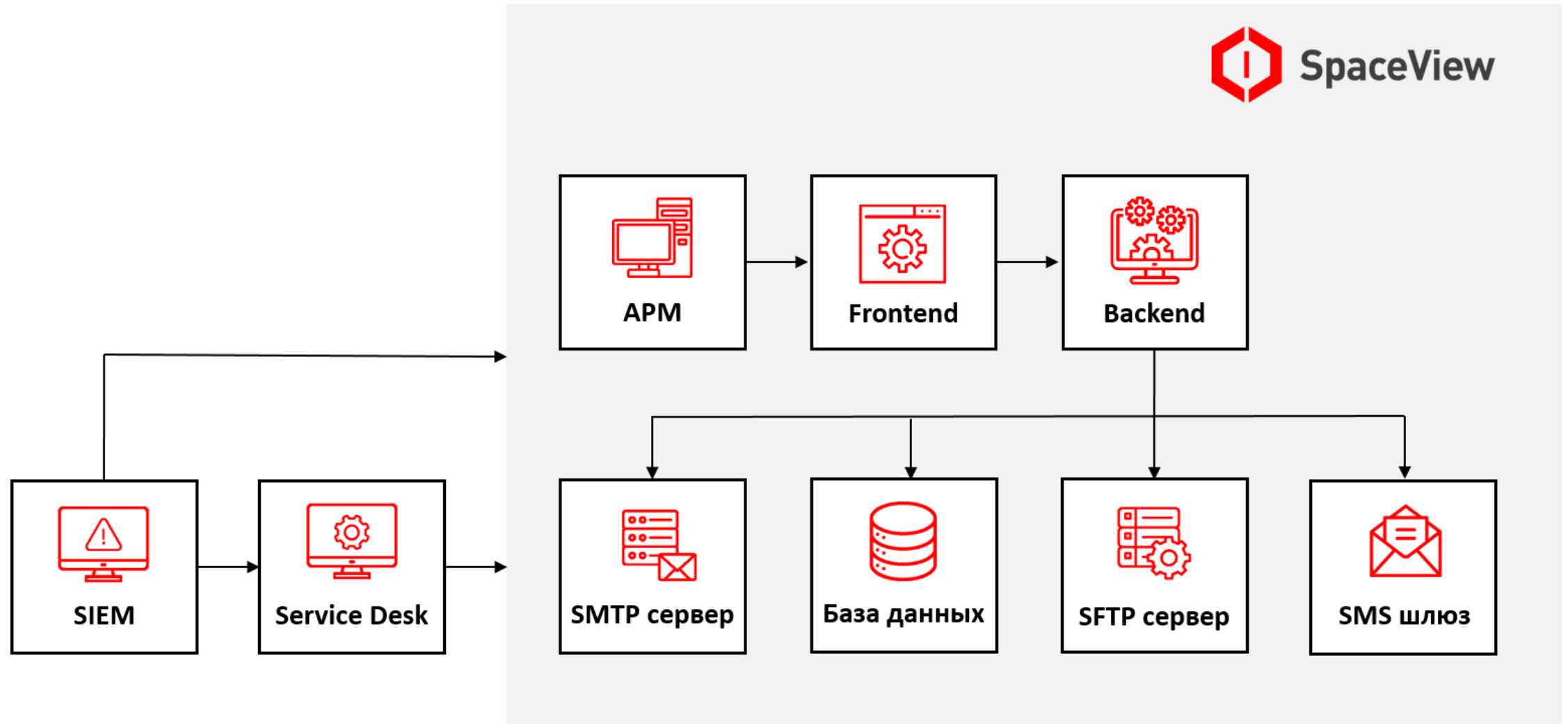


Оперативная техподдержка



Российская разработка

Архитектура SpaceView



Возможности интеграции

- Интеграция с популярными SIEM (IBM Qradar, PT MaxPatrol и др.)
- Интеграция с Jira ServiceDesk
- Оперативная реализация интеграций с системами Заказчика
- Подключение к SIEM напрямую или через Service Desk

Подключение через Service Desk дает дополнительные преимущества: предварительная аналитика и отбор, возможность пополнения БЗ, возможность передачи в SpaceView только отобранных офицером безопасности инцидентов и т.д.

Интерфейсы SpaceView. Работа с инцидентами

The screenshot shows the SpaceView interface with a sidebar on the left containing navigation options: Инциденты, Заявки, Отчёты, Показатели за неделю, Управление инцидентами, Статистика инцидентов ИБ, Контроль источников, Статистика источников, Организации, Пользователи, Ресурсы, Справочники, and Новости. The main area displays a table of incidents with columns for ID, Name, Type, and Status.

ID	Наименование	Тип	Статус
Test files		Инцидент	Новый
rega	Обнаружено добавление записи в реестр на автозапуск исполняемого файла, ранее не замеченного в организации	Инцидент	Проведено расследование
	Обнаружено подозрительное создание исполняемого файла через SMB и System	Инцидент	Закрыт
	Обнаружено RDP/TCP соединение от необычного процесса	Инцидент	Закрыт
	Обнаружен вирус на хосте	Инцидент	Закрыт
	Обнаружен потенциально злонамеренный доступ к процессу Isass	Инцидент	Закрыт
	Пользователь был добавлен в привилегированную группу Local	Инцидент	Закрыт
	Обнаружено открытие портов через Microsoft Firewall	Инцидент	Закрыт
	Обнаружен перебор паролей для одной УЗ Windows	Инцидент	Закрыт

Атрибуты

№	Наименование	Значение
1	Source Name	WIN-07-Oleg
2	Source IP	192.168.0.33
3	Destination Name	MYHOST-W10-TC
4	Destination IP	192.168.0.220
5	User Name	Oleg
6	Destination Port	3389

Комментарии

Адаев Никита
25.05.2021 в 16:15 с хоста WIN-07-Oleg(IP - 192.168.0.33) зафиксировано сетевое соединение с хостом MYHOST-W10-TC (IP - 192.168.0.220) по протоколу RPD. Инициатор активности - C:\Users\Oleg\AppData\Local\minecraft.exe, запущенный под учетной записью Oleg. По данным TI хеш данного процесса вредоносный. Коллеги, просьба предоставить файлы с папки C:\Users\Oleg\AppData\Local в IZ:SOC.

ID	Наименование	Тип	Проведение расследования	Степень	Дата и время	Исполнитель	Организация
DEMO-10	gers	Инцидент	Проведение расследования	Низкий	02.12.2021 16:31	Козлов Роман Андреевич	АО "Демостенд"
DEMO-9	Обнаружено добавление записи в реестр на автозапуск исполняемого файла, ранее не замеченного в организации	Инцидент	Закрыт	Критичный	25.05.2021 13:48	Долматов Денис Викторович	АО "Демостенд"
DEMO-8	Обнаружено подозрительное создание исполняемого файла через SMB и System	Инцидент	Закрыт	Критичный	24.05.2021 16:51	Долматов Денис Викторович	АО "Демостенд"
DEMO-7	Обнаружено RDP/TCP соединение от необычного процесса	Инцидент	Закрыт	Средний	24.05.2021 16:32	Адаев Никита	АО "Демостенд"
DEMO-6	Обнаружен вирус на хосте	Инцидент	Закрыт	Средний	21.05.2021 17:57	Адаев Никита	АО "Демостенд"
DEMO-5	Обнаружен потенциально злонамеренный доступ к процессу Isass	Инцидент	Закрыт	Средний	21.05.2021 16:12	Адаев Никита	АО "Демостенд"
DEMO-4	Пользователь был добавлен в привилегированную группу Local	Инцидент	Закрыт	Средний	21.05.2021 15:58	Долматов Денис Викторович	АО "Демостенд"
DEMO-3	Обнаружено открытие портов через Microsoft Firewall	Инцидент	Закрыт	Средний	21.05.2021 15:54	Адаев Никита	АО "Демостенд"

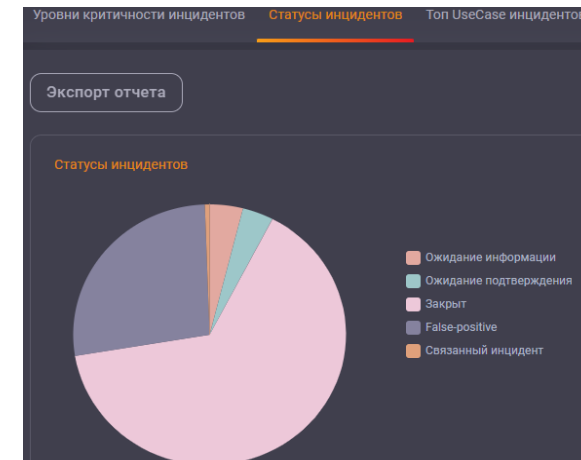
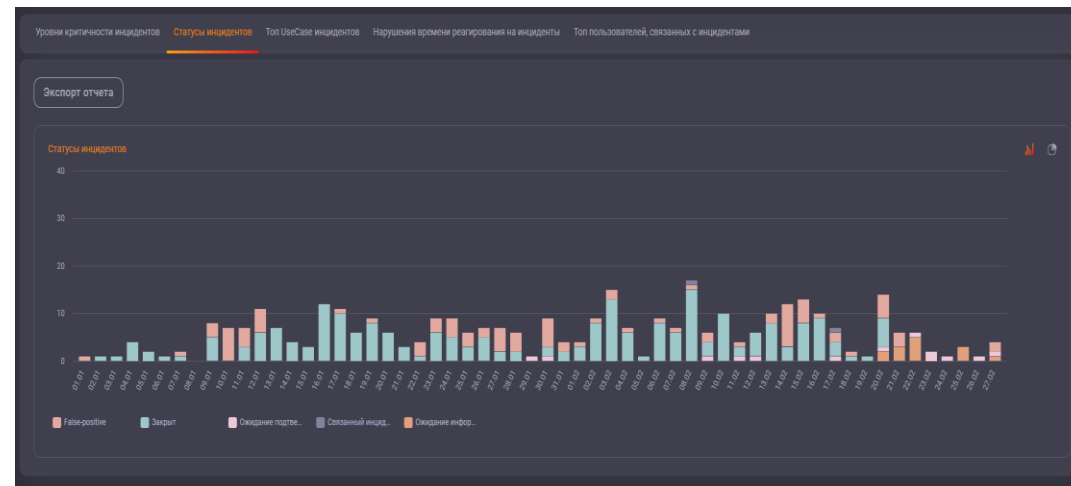
Интерфейсы SpaceView. Настройка правил

The screenshot displays the SpaceView web interface for configuring rules. The main header includes the SpaceView logo, a search icon, a language dropdown set to 'РУС', and the user profile 'Зиятдинов Azat, Администратор'. The left sidebar is titled 'Информзащита' and contains tabs for 'Свойства', 'Категории заявок', and 'Правила'. The 'Правила' tab is active, showing a list of existing rules with columns for 'Наименование' and 'Подсеть'. The main content area is titled 'Создание правила' and contains the following fields:

- Наименование:** Подсеть 192.168.1.0/24
- Атрибуты:** Выбрано (1)
- UseCase:** Внутренние сканирование сети (Priority: Низкий)
- UseCase:** Внешнее сканирование сети (Priority: Критичный)
- Паттерн:** 192.168.1.55
- Паттерн:** 192.168.1.56

Buttons for 'Добавить', 'Сохранить', and 'Отменить' are visible at the bottom of the configuration panel.

Интерфейсы SpaceView. Отчетность



О компании Spacebit

Spacebit - российский разработчик современных программных продуктов в области информационной безопасности. Компания создает эффективные инструменты, помогающие бизнесу и государственным организациям различного масштаба повышать уровень защищенности ИТ-инфраструктуры и автоматизировать процессы управления ИБ.



Решения



Система управления
уязвимостями конфигураций
информационных ресурсов



Система управления
жизненным циклом средств
криптографической защиты
информации



Система мониторинга и
реагирования на инциденты
информационной
безопасности

Наши преимущества



Российская разработка

все продукты создаются на территории РФ и включены в Реестр отечественного ПО



Универсальность применения

решения подходят для любых организаций вне зависимости от отрасли и масштаба



Простота развертывания и обслуживания

продукты быстро интегрируются в ИТ-инфраструктуру и легко поддерживаются



Гибкость и масштабируемость

системы масштабируются и кастомизируются под бизнес-требования заказчика



Политика лицензирования

модель лицензирования позволяет подобрать оптимальное решение для каждой компании



Оперативная техподдержка

специалисты помогут решить любые вопросы по настройке, эксплуатации и обновлению систем

Наши партнеры

softline[®]

itprotect

T.Hunter

КРОК



Информзащита
Системный интегратор

КРОСС
ТЕХНОЛОДЖИС



АСТЕРИТ
Безопасность информационных
технологий

ARinteg[®]
ВАШ ГАРАНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



IT TASK
системный интегратор



ТАЛМЕР
системная интеграция



BUSINESS IT

СИСТЕМАТИКА

**ИМПУЛЬС
ТЕЛЕКОМ**



Open Vision
technology in detail

СИССОФТ

Контакты

SPACE·BIT



www.spacebit.ru



info@spacebit.ru



+7 (495) 989-90-01

