

АМ IMS 3.0: Управление инцидентами информационной безопасности

Артём Савчук
Технический директор
«Перспективный мониторинг»

БОЛЬШОЙ
МОСКОВСКИЙ
ТЕХНО  infotecs
Фест

AM Incident Management System

Система управления инцидентами является «службой одного окна» для всех специалистов, задействованных в процессе управления инцидентами ИБ, удобной как для работников Центра мониторинга, так и для специалистов Заказчика.

Включено в реестр отечественного ПО, реестровая запись №29485 от 29.08.2025

РОССИЙСКАЯ ФЕДЕРАЦИЯ RU 2023614105

 incident management

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства): 2023614105	Правообладатель: АКЦИОНЕРНОЕ ОБЩЕСТВО « ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ» (АО «ПМ») (RU)
Дата регистрации: 22.02.2023	
Номер и дата поступления заявки: 2023611118 24.01.2023	
Дата публикации: 22.02.2023	
Контактные реквизиты: +79264256054, pavel.kononov@amonitoring.ru	

Название программы для ЭВМ:
«Система управления инцидентами информационной безопасности AM Incident Management System»

Реферат:
Программа предназначена для регистрации, учёта и обработки инцидентов информационной безопасности. Позволяет автоматизировать деятельность по управлению жизненным циклом инцидентов ИБ; классификация, приоритизация, эскалация инцидентов ИБ; агрегация информации по инцидентам ИБ; формирование отчётности; автоматизированный обмен информацией с регуляторами и внешними СЗИ. ОС: Windows, GNU/Linux, macOS.

Возможности

AM Incident Management System



Управление
инцидентами ИБ



Обмен информацией
об угрозах ИБ



Учёт
ИТ-активов



Построение статистических
графиков, дашбордов



Формирование
отчётности



Работа с организациями
и филиалами

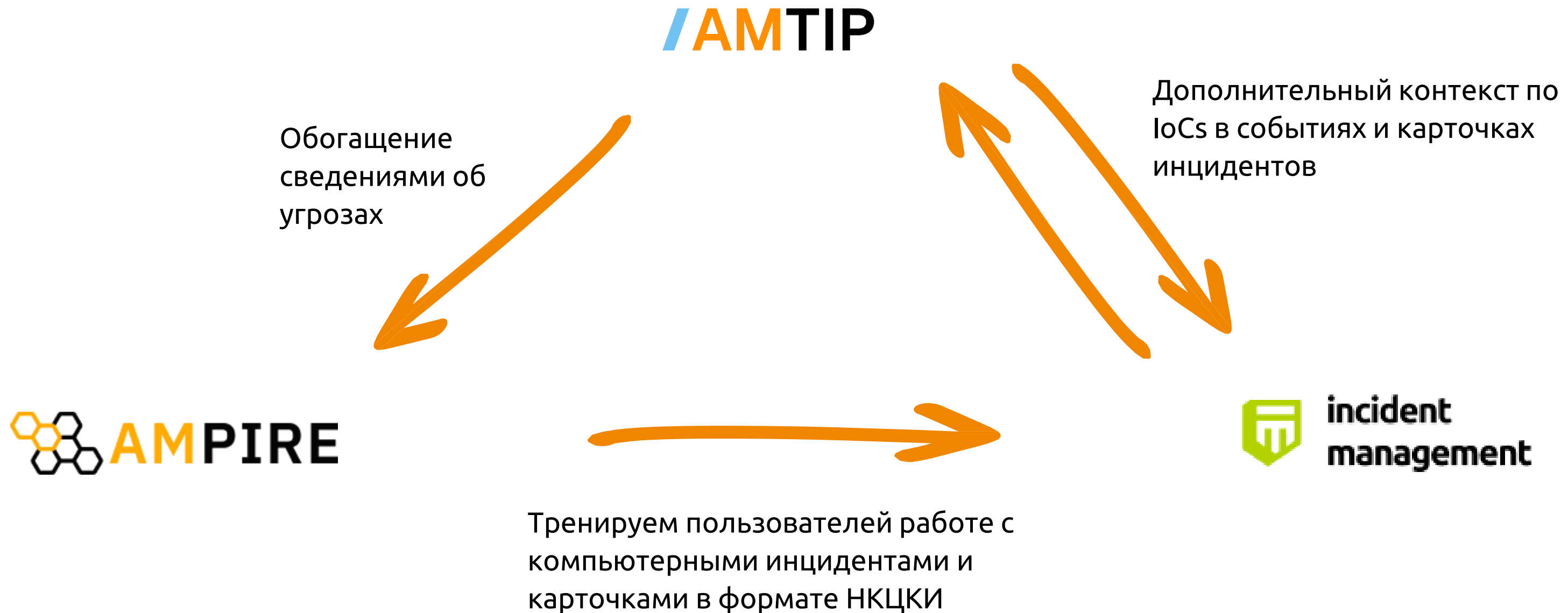


Интеграция с
ГосСОПКА



Оперативное оповещение
по e-mail, telegram, sms

Экосистема продуктов ПМ



Управление инцидентами ИБ*

АМ IMS применяется:

- **На этапе планирования и подготовки** - для формализации политик ИБ, информирования пользователей;
- **На этапе использования** – для создания, оповещения, расследования и реагирования на инциденты ИБ;
- **На этапе анализа** – для обобщения, анализа и систематизации информации об инцидентах ИБ;
- **На этапе улучшения** – для уточнения результатов и улучшения системы менеджмента инцидентов ИБ.

* - ГОСТ Р ИСО/МЭК ТО 18044-2007

Управление КИ для субъектов ГосСОПКА



ГОСТ Р 59710-2022 регулирует управление КИ для:

- субъектов ГосСОПКА, осуществляющих управление КИ в отношении собственных информационных ресурсов;
- центров ГосСОПКА, в зону ответственности которых входят информационные ресурсы других субъектов ГосСОПКА.

Соответствие ИМ требованиям ГОСТ Р 59710–2022



Требование	АМ IMS	Примечание
Организация деятельности по управлению КИ		
Разработка политики управления КИ	Помогает	Раздел «Документация» позволяет сформировать базу знаний на основе ПИБ Компании.
Разработка плана реагирования на КИ		
Определение подразделения, ответственного за управление КИ	Помогает	При создании пользователя задается соответствующая ему роль в системе
Организация взаимодействия с подразделениями внутри организации и с внешними организациями	Позволяет	Диспетчеризация внутри системы + API
Материально-техническое оснащение подразделения, ответственного за управление КИ	Не позволяет	
Организовать обучение и информирование в части управления КИ		Может быть реализовано на киберполигоне Ampire
Проведение тренировок по отработке мероприятий плана реагирования на КИ		
Обнаружение и регистрация КИ		
Регистрация признаков возможного возникновения компьютерных инцидентов	Позволяет	В разделе «Инциденты» возможно создавать карточки КИ и КА, при закрытии инцидента указывается признак True/False positive
Подтверждение компьютерных инцидентов	Позволяет	

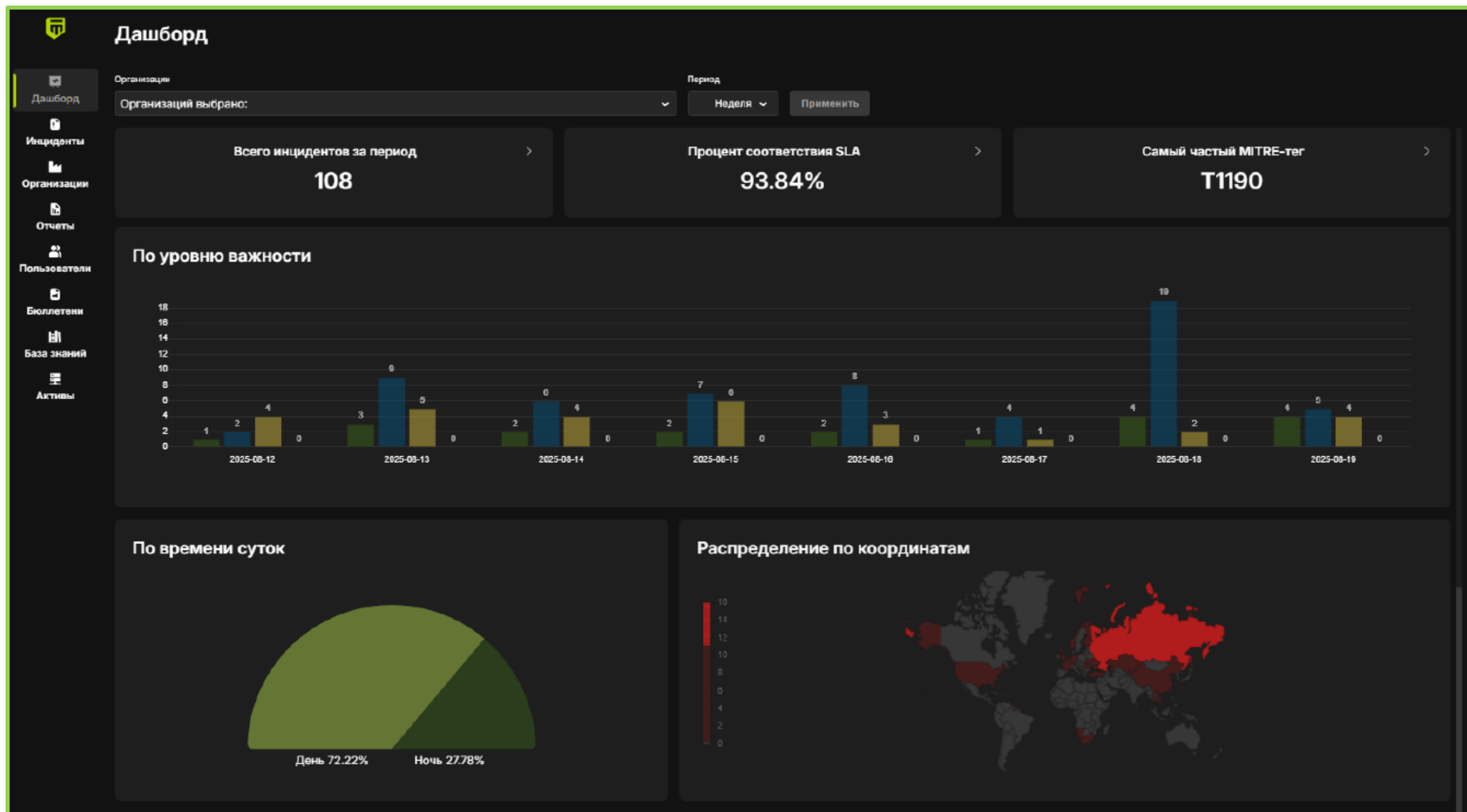
Соответствие ИМ требованиям ГОСТ Р 59710–2022



Требование	АМ IMS	Примечание
Реагирование на компьютерные инциденты		
Определение вовлеченных в КИ элементов информационной инфраструктуры	Позволяет	Раздел «Активы» позволяет вести учет ИТ-активов организации
Выявление последствий КИ	Позволяет	Функция «Проверка активности» позволяет проверить полноту реагирования
Ликвидация последствий КИ	Помогает	Выполняется вне ИС по указанным в карточке КИ/КА шагам (runbooks)
Локализация КИ		
Заккрытие КИ	Позволяет	Обработанные инциденты Переходят в статус «Закрит»
Фиксация материалов, связанных с возникновением компьютерного инцидента	Позволяет	Вкладка «Файлы» в карточке КИ позволяет крепить цифровые следы
Установление причин и условий возникновения компьютерного инцидента	Позволяет	Вкладка «События» и история карточки КИ
Анализ результатов деятельности по управлению КИ		
Приобретение и накопление опыта по результатам управления КИ	Позволяет	В разделе «Документация» возможно добавлять статьи с разбором кейсов
Разработка рекомендаций по устранению в ИР причин и условий возникновения КИ	Помогает	Карточки КИ/КА, извлечение уроков, playbooks для аналогичных кейсов
Оценка результатов и эффективности реагирования на КИ	Позволяет	«Дашборд» позволяет просматривать статистику и SLA по зарегистрированным инцидентам

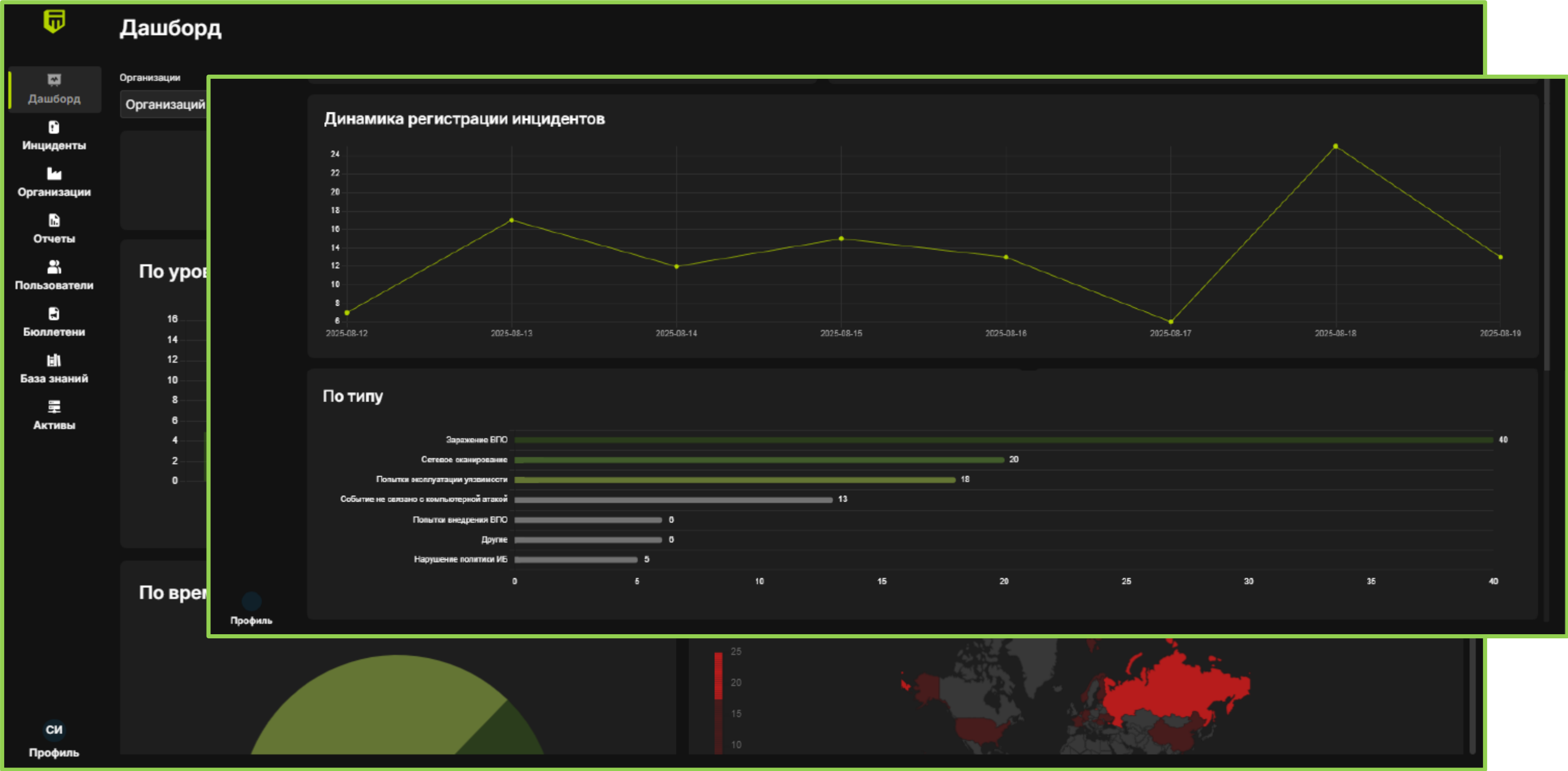


Построение статистических графиков, дашбордов



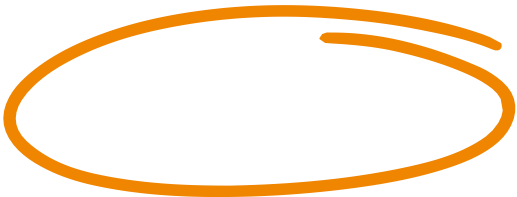


Построение статистических графиков, дашбордов





Управление инцидентами ИБ
Раздел «Инциденты»



Дашборд

Инциденты

Организации

Отчеты

Пользователи

Бюллетени

База знаний

Активы

Инциденты

Hrid	Название	Статус	Регистрационный номер НКЦКИ	Статус уведомления НКЦКИ
	Подозрение на XServer/Agent на узле 10.139.12.71	В работе у ЦМ		Неизвестно
	Недоступность веб-ресурсов slots.rmiac18.ru, monlek.rmiac18.ru	В работе у клиента		Неизвестно
	Подозрительная активность, связанная с ВПО SocGholish, от узла 192.168.38.150	В работе у клиента		Неизвестно
	Активность сканера Nmap от узла 192.168.153.106	В работе у клиента		Неизвестно
	Подозрительная активность, связанная с Watch Wolf, от узла 192.168.0.4	В работе у клиента		Проверка НКЦКИ
	Подозрительная активность, связанная с ВПО Balada Injector, от узла 192.168.161.89	В работе у клиента		Проверка НКЦКИ
	Потенциально нежелательное ПО Tool.KMS, Tool.Hstart на узле srmед	В работе у клиента		Неизвестно
	Сканирование на наличие уязвимости CVE-2021-44228 от узла 85.142.100.82	Закрыт		Неизвестно
	Потенциально нежелательное ПО Tool.KMS на узле DESKTOP-9HI7AOR	В работе у клиента		Неизвестно
	Множественные попытки авторизации от узла 10.0.10.184 защищаемой сети	В работе у клиента		Неизвестно

Добавить инцидент

Пресеты Столбцы Фильтр

Организация

Перспективный мониторинг

Тип инцидента

Заражение ВПО

Регистрация с

Не выбрано

Регистрация по

Не выбрано

Линия

Первая линия

Вторая линия

Статус

В работе у ЦМ

В работе у клиента

Запрос на закрытие

Закрыт

Статус НКЦКИ

Создано

Зарегистрировано

Требуется дополнение

Проверка НКЦКИ

Принято решение

Отправлено в архив

Сбросить

Применить



Управление инцидентами ИБ

Карточка КИ/КА



Подозрительная активность на узле 10.10.44.204

HRID: AM-15 Создан: 2025-04-03 17:14:27 Обновлено: 2025-04-04 11:21:51 Просмотрен: 2025-04-04 12:37:47

Отправлен клиенту

Основное События История Чат

Рекомендации

- ☐ Заблокировать адрес источника 134.175.121.153.
- ☐ Провести антивирусную проверку. Антивирус должен иметь актуальные базы сигнатур.
- ☐ Если установленный антивирус отсутствует, в безопасном режиме провести сканирование узла антивирусным средством KVRT от Kaspersky Lab последней версии с актуальными базами.

Предпринятые действия

Предпринятые действия отсутствуют

Ручная проверка активности

Активности нет

Файлы

(Китай, ISP:TENCENT-CN, ASN:45090) сети Интернет, зафиксированного во многих черных списках вредоносной активности. Данная активность может свидетельствовать о наличии backdoor на узле 10.10.44.204 защищаемой сети. Meterpreter — это многофункциональная полезная нагрузка, которая используется в Metasploit Framework как основа для постэксплуатации. Backdoor — это тип вредоносного программного обеспечения, который позволяет злоумышленнику получить несанкционированный доступ к системе или сети,



Интеграция с
ЛК ГосСОПКА



Попытки внедрения PHP-инъекций

HRID: RICUR-2405

НКЦ

Регист
WRN

Уведомление Комментарии Свидетельства История

Категория **Общие сведения** Контролируемый ресурс Технические сведения

Общие сведения

Регистрационный номер

WRNG-25-03-6278

Статус уведомления

Отправлено в архив

Тип инцидента

15

Компания

АУ УР "РИЦ УР"

Владелец информационного ресурса

АУ УР "РИЦ УР"

Статус реагирования

Проводятся мероприятия по реагированию

☐ Требуется содействие НКЦКИ

Выявлен

Не выбрано

Закрит

Не выбрано

Средство выявления

ViPNet IDS NS

TLP

TLP:AMBER

Описание

В ходе ретроспективного анализа зафиксированы попытки внедрения PHP-кода на ресурсы защищаемой сети.

Влияние на целостность

Ничего не выбрано

Влияние на доступность

Ничего не выбрано

Влияние на конфиденциальность

Ничего не выбрано



Работа с организациями и филиалами



Организация

ПМ

К

Д

А

Перспективный мониторинг

О компании

Технические сведения

Пользователи

Основная информация

☐ Является СКИИ

☒ Первая линия ЦМ

☒ Активная

Префикс

am

Копировать

Короткое название

АО "ПМ"

Юридическое название

Перспективный мониторинг

Е-mail

Ничего не выбрано

Временная зона

(UTC+03:00) Москва, Санкт-Петербург

Адрес

Ничего не введено

Создана: 2022-08-24 11:33:21 Обновлено: 2023-07-03 19:41:24 Деактивирована: -

НКЦКИ

Контракт

Организацию

исей: 2



Формирование отчётности



Отчет

Дашборд

Инциденты

Организации

Отчеты

Пользователи

Бюллетени

База знаний

Активы

СИ

Профиль

ГК ИнфоТ

Дата созд

2023-12 18:56

2023-10 19:03

2023-11 19:17

2024-04 15:20

2024-04 15:21

2024-04 15:22

2024-04 15:23

2024-05 15:02

2024-07 14:22

2024-07 14:22

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Отчёт
по обнаруженным
инцидентам ИБ

01.01.2025 - 31.01.2025

Добавить отчет

РЕЗЮМЕ

За отчётный период с 01.03.2025 по 31.03.2025 в организации
выявлено **11** компьютерных инцидентов и **6** компьютерных атак.
Также выявлено **0** компьютерных уязвимостей.

КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ				КОМПЬЮТЕРНЫЕ АТАКИ			
11				6			
РАСПРЕДЕЛЕНИЕ ПО ВРЕМЕНИ СУТОК							
ДЕНЬ	100.0%	НОЧЬ	0.0%	ДЕНЬ	100.0%	НОЧЬ	0.0%
ДОЛЯ КРИТИЧЕСКИХ							
0.0%				0.0%			
ПРОДОЛЖАЕТСЯ РАБОТА							
5				0			
В РАБОТЕ У ЗАКАЗЧИКА							
5				0			

Среднее время регистрации инцидента ИБ специалистом ЦМ АО «ПМ» с момента выявления составило **01:20:54**

Среднее время решения инцидентов ИБ составило **1 д. 15:51:14**

Среднее время реакции клиента (Заказчика) **02:38:52**

Среднее время принятия мер реагирования **21:19:57**

Среднее время выработки мер реагирования **00:04:28**

Среднее время нахождения в работе у Клиента **5 д. 16:58:12**



Учёт ИТ-активов



Активы

Сегменты Сети Узлы

Организации

🔍 пер 🔴 Фильтр ▾

Название организации

Демонстрационный стенд Перспективный Мо...

✕ Esc

Хост	Домен	
uuu	uuu.ru	
IP адреса	MAC адреса	IP адреса шлюза
91.244.183.5 x ▾	f0:98:9d:1c:93:f7 ▾	91.244.183.1 ▾
Категория обрабатываемых данных	Тип обрабатываемых данных	
Открытая информация ▾	Официально публикуемая ин... ▾	
Сети		
Демосеть ▾		
Адрес		
kjhkjlh		
Операционная система	Оценочная стоимость	
Microsoft Windows Server ▾	9898.00	
Источник информации		
Инвентаризационные данные ▾		
Критичность		
☐ Низкая ☐ Средняя ☒ Высокая		
☐ Доступ к сети ☐ Является КИИ		



Обмен информацией об угрозах ИБ
Бюллетени



Бюллетени

Поиск

Дата регистрации ↓	Название ↓
2024-06-26	Угроза рас
2024-06-18	SQL-инъекц
2024-06-17	Множествен
2024-06-03	Общедоступ
2024-05-28	Удаленное и
2024-04-02	Библиотека
2024-03-16	Угроза рас
2024-03-11	Информаци
2024-03-05	Уязвимость
2024-03-04	Бюллетень с

Отчет о прочтении: SQL-инъекция в Zabbix

Пользователь	Дата и время скачивания	Дата и время прочтения
...	2024-06-21 10:01:05	-
...	2024-06-24 09:39:58	2024-06-24 09:40:02
...	2024-07-08 10:09:19	-
...	2024-07-10 11:30:42	-
...	2024-07-12 07:38:31	2024-07-12 07:38:36
...	2024-07-26 05:51:06	2024-07-26 05:52:28
...	2024-08-01 08:34:25	-
...	2024-08-09 15:43:37	-
...	2024-09-02 07:32:24	-
...	2024-09-12 08:09:53	-

Бюллетень

записей: 26

Действия

📄

🗑

📄

🗑

📄

🗑

📄

🗑

📄

🗑

📄

🗑

📄

🗑

📄

🗑

📄

🗑

📄

🗑



Обмен информацией об угрозах ИБ
с **AMTIP**



Дашборд

Инциденты

Организации

Отчеты

Пользователи

Бюллетени

База знаний

Активы

АВ

Профиль

Обращения на killswitch домен Wannacry

HRID: 329428394 | Создан: 12.04.23 09:33 | Изменен: 12.04.23 09:33 | Просмотрен: 12.04.23 09:33

ОсновноеСобытияИсторияЧатIOCSЗатронутые активы

Индикаторы

Тип	IOC	AM Score	Дата обновления	Score
CVE		0.60	12.03.23 17:56	
CVE		0.60	12.03.23 17:56	
URL		0.60	12.03.23 17:56	
IP-адрес		0.60	12.03.23 17:56	
Домен		0.60	12.03.23 17:56	
Хэш	b034c15f75	0.60	12.03.23 17:56	
Иная		0.60	12.03.23 17:56	

Спасибо за внимание!



t.me/pm_public



[@AMonitoring](https://www.youtube.com/@AMonitoring)



amtip.ru

Артём Савчук

Технический директор

+7 (495) 737-61-97

info@amonitoring.ru

ТЕХНО infotecs Фест

Подписывайтесь
на наши соцсети,
там много интересного



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

