



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Подключение к ГосСОПКА

Роман Кобцев

Директор по развитию бизнеса ЗАО «Перспективный
мониторинг»



Компоненты работающего решения

- Нормативная база
- Технические аспекты подключения
 - Выполняемые функции
 - Ресурсы
 - Обмен сведениями
- Применение на практике



Нормативная база

Что читать

Нормативные правовые акты



- **Основные направления государственной политики** в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом РФ 03.02.2012 N 803)
- **Концепция** государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом РФ 12 декабря 2014 г. N К 1274)

Нормативные правовые акты



- **Указ Президента Российской Федерации от 22.12.2017 г. № 620** О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (По сути сменил Указ Президента РФ от 15 января 2013 г. N 31с)
- **Федеральный закон от 26.07.2017 N 187-ФЗ** «О безопасности критической информационной инфраструктуры Российской Федерации»

Приказы ФСБ России.

(Зарегистрированы в Минюсте 6 сентября 2018)



- **Приказ ФСБ России от 24 июля 2018 г. № 366** «О Национальном координационном центре по компьютерным инцидентам (НКЦКИ)»
- **Приказ ФСБ России от 24.07.2018 № 367** "Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации«
- **Приказ ФСБ России от 24 июля 2018 г. № 368** «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

Приказы ФСБ России. (Опубликованные проекты)



- **Проект приказа ФСБ России** «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»
- **Проект приказа ФСБ России** «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»
- **Проект приказа ФСБ России** «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ»

Методические документы ФСБ России.



- Методические рекомендации ФСБ России по созданию ведомственных сегментов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
- Методические рекомендации ФСБ России по обнаружению компьютерных атак на информационные ресурсы Российской Федерации
- Методические рекомендации ФСБ России по установлению причин и ликвидации последствий компьютерных инцидентов связанных с функционированием информационных ресурсов Российской Федерации
- Методические рекомендации НКЦКИ по проведению мероприятий по оценке степени защищенности от компьютерных атак.
- ТРЕБОВАНИЯ к подразделениям и должностным лицам субъектов ГОССОПКА
- РЕГЛАМЕНТ взаимодействия подразделений ФСБ и субъекта ГОССОПКА при осуществлении информационного обмена в области обнаружения предупреждения и ликвидации последствий компьютерных атак



А это обязательно?

187-ФЗ

Статья 9. Права и обязанности субъектов критической информационной инфраструктуры

Субъект критической информационной инфраструктуры обязан незамедлительно информировать о компьютерных инцидентах соответствующие федеральные органы исполнительной власти (НКЦКИ ГосСОПКА, а также Финцерт ЦБ РФ для финансовых организаций), а также реагировать на компьютерные инциденты в установленном порядке.

Перечень сведений, предоставляемых в ГосСОПКА



Приказ ФСБ России № 367

от 24 июля 2018 г.

«Об утверждении Перечня

информации,

представляемой в ГосСОПКА

и Порядка представления

информации в ГосСОПКА»

- О категорировании объекта
- О нарушении требований по обеспечению безопасности значимых объектов КИИ (по итогам проведения государственного контроля)
- Информация о компьютерных инцидентах, связанных с функционированием объектов КИИ
- Иная информация в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.



Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

Два способа предоставления информации в НКЦКИ:

- с использованием технической инфраструктуры НКЦКИ
- посредством электронной, факсимильной, почтовой и телефонной связи.

ГосСОПКА это не только КИИ



ОГВ

Могут быть
подключены к
ГосСОПКА



КИИ

Обязаны быть
подключены к
ГосСОПКА





ГосСОПКА – территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Зона ответственности – совокупность информационных ресурсов, в отношении которых субъектом ГосСОПКА обеспечиваются обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

Субъекты ГосСОПКА – государственные органы Российской Федерации, российские юридические лица и индивидуальные предприниматели в силу закона или на основании заключенных с ФСБ России соглашений осуществляющие обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

Центр ГосСОПКА – структурная единица ГосСОПКА, представляющая совокупность подразделений и должностных лиц субъекта ГосСОПКА, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и реагирование на компьютерные инциденты в своей зоне ответственности.

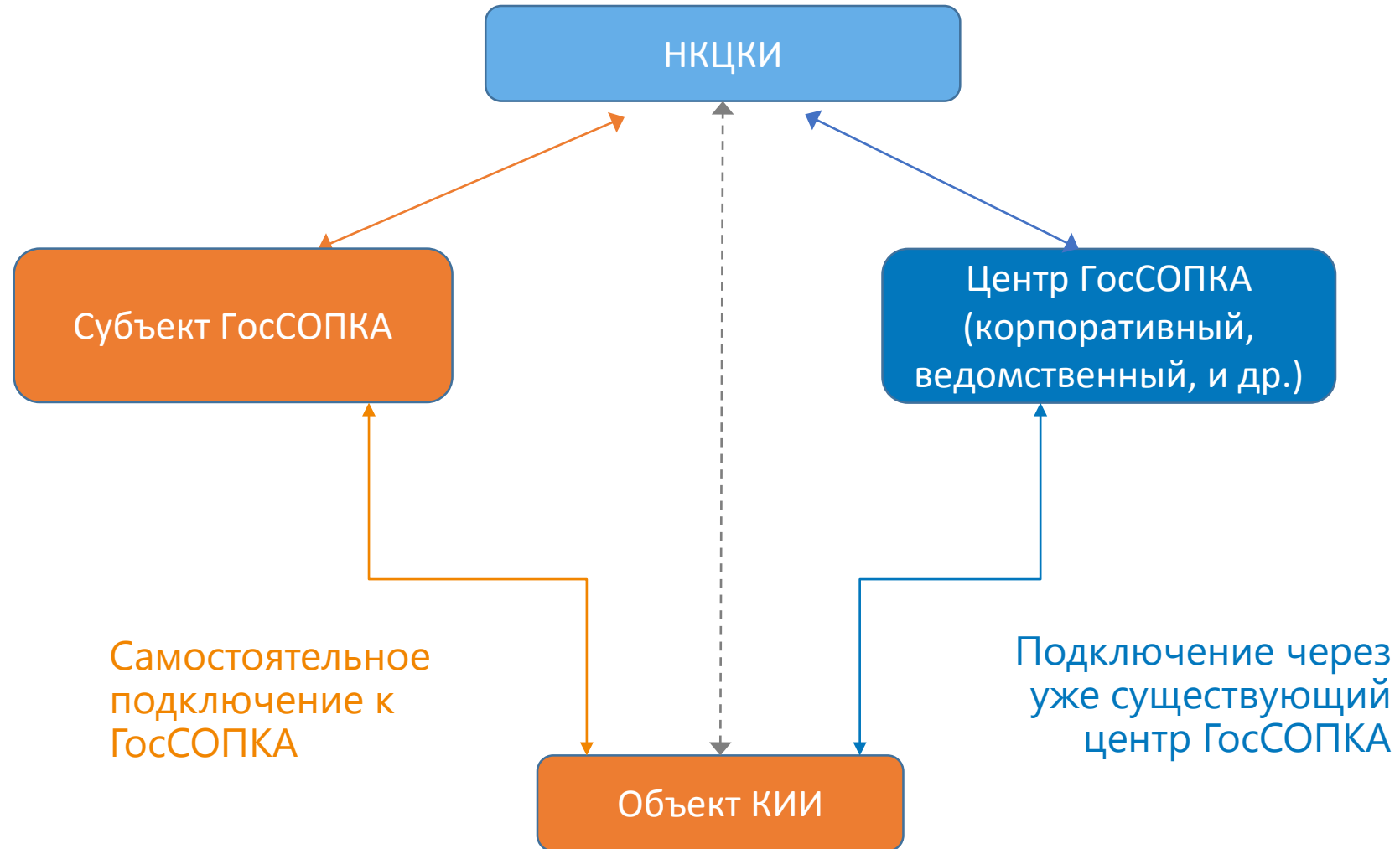


Технические аспекты

Что делать



ГОССОПКА



Что делать?



В случае самостоятельного подключения к ГосСОПКА

- ✓ Обеспечить взаимодействие с 8Ц ФСБ России
- ✓ Выполнить организационные и технические требования в соответствии с нормативными правовыми актами и методическими рекомендациями
- ✓ Развернуть специализированные системы взаимодействия с технической инфраструктурой НКЦКИ (для значимых КИИ обязательно, остальным опционально).

В случае подключения через сторонний корпоративный сегмент

- ✓ Заключение соглашения с корпоративным центром
- ✓ Уведомить НКЦКИ о включении своих информационных ресурсов в зону ответственности корпоративного центра.



Какие функции выполняют центры ГосСОПКА

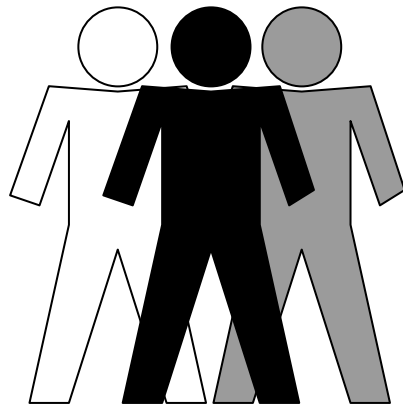
Функции	Центры ГосСОПКа		
	Класса А	Класса Б	Класс В
а) взаимодействие с НКЦКИ при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и реагирования на компьютерные инциденты, в том числе в части информационно-аналитического и прогностического обеспечения функционирования ГосСОПКА, предоставление в НКЦКИ сведений о состоянии защищенности информационных ресурсов от компьютерных атак и информации о компьютерных инцидентах в соответствии с установленным порядком;	+	+	+
б) разработка документов, регламентирующих процессы обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов и реагирования на компьютерные инциденты;	+	+	+
в) эксплуатация средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, выявление ошибок в работе средств и направление производителю средств информации о выявленных ошибках, а также актуализация средств используемых для обеспечения защиты информационных ресурсов, направление в НКЦКИ предложений по совершенствованию средств;	+	+	+
г) прием сообщений об инцидентах от персонала и пользователей информационных ресурсов;	+	+	+
д) регистрация компьютерных атак и компьютерных инцидентов;	+	+	+
е) анализ событий информационной безопасности;	+	+	+
ж) инвентаризация информационных ресурсов;	+	+	+
з) анализ угроз информационной безопасности, прогнозирование их развития и направление в НКЦКИ результатов;	+	+	
и) составление и актуализация перечня угроз информационной безопасности для информационных ресурсов;	+	+	
к) выявление уязвимостей информационных ресурсов;	+	+	
л) формирование предложений по повышению уровня защищенности информационных ресурсов;	+	+	
м) составление перечня последствий компьютерных инцидентов;	+	+	
н) ликвидация последствий компьютерных инцидентов;	+		
о) анализ результатов ликвидации последствий инцидентов;	+		
п) установление причин компьютерных инцидентов.	+	+	

Необходимые ресурсы



Силы ГосСОПКА

Средства ГосСОПКА



Кадровое обеспечение

Средства
обнаружения,
средства
предотвращения,
средства ликвидации
последствий



Практическое применение

Как это работает

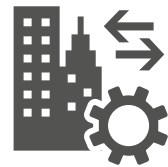
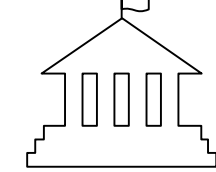


Инвентаризация

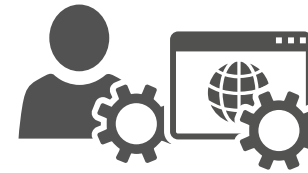
Главный центр
ГосСОПКА



Корпоративный центр
мониторинга



Анализ



Перечень ПО, обновления,
настройки, сервисы



Реагирование



Контролируемая
инфраструктура заказчика

Система инвентаризации



Inventory System

Search

REPORTS

JSON

Advanced Monitoring resources list

Host Name	Timestamp	os_version	arch
MSK-W0038		Корпоративная	64-разрядная
MSK-W0057		Корпоративная	64-разрядная
MSK-W0326		Корпоративная	64-разрядная
MSK-W0603		Корпоративная	64-разрядная
MSK-W1595	1515745810	Майкрософт Windows 10 Корпоративная	64-разрядная

Наименование и характеристики ресурса

MSK-W0038 Software List

Application Name	Version	CVE count	Approve
		0	X
		0	✓
		0	✓
		2	✓
Adobe Reader XI (11.0.23) MUI	11.0.23	26	✓

Наименование и версия ПО

Selected: Adobe Reader XI (11.0.23) MUI

cpe:"cpe:/a:adobe:acrobat_reader"

cve:26

- ! CVE-2013-3346 (cvss:10)
- ! CVE-2013-3342 (cvss:10)
- ! CVE-2013-3341 (cvss:10)
- ! CVE-2013-3340 (cvss:10)
- ! CVE-2013-3339 (cvss:10)
- ! CVE-2013-3338 (cvss:10)
- ! CVE-2013-3337 (cvss:10)
- ! CVE-2013-2736 (cvss:10)

Сведения по уязвимостям



**Ввод в
эксплуатацию**

Ежемесячно

Ежеквартально

Ежегодно

анализ
документации

сетевое и
системное
сканирование

контроль
устранения ранее
выявленных
уязвимостей

тестирование на
проникновение

анализ исходного
кода

контроль
выполнения
требований
безопасности

оценка
соответствия мер
защиты

Система управления уязвимостями



- Анализ в реальном времени
- Экспертная поддержка
- Интерфейс взаимодействия для обработки уязвимостей и принятия решений



Обработка уязвимостей

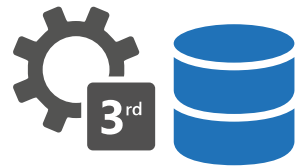


Публичные
базы
уязвимостей

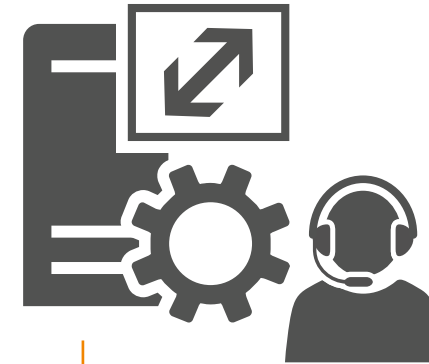


bdu.fstec.ru

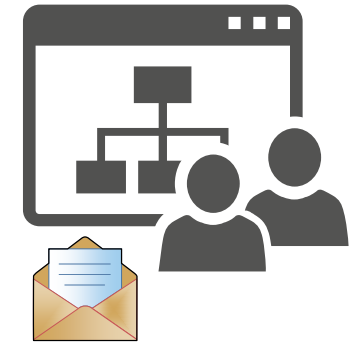
Обработка,
агрегация и
формирование
базы уязвимостей



ИАЦ



Пользователи
Реагирование



Сопоставление данных

Хранение сведений 3 года

Обработка уязвимостей



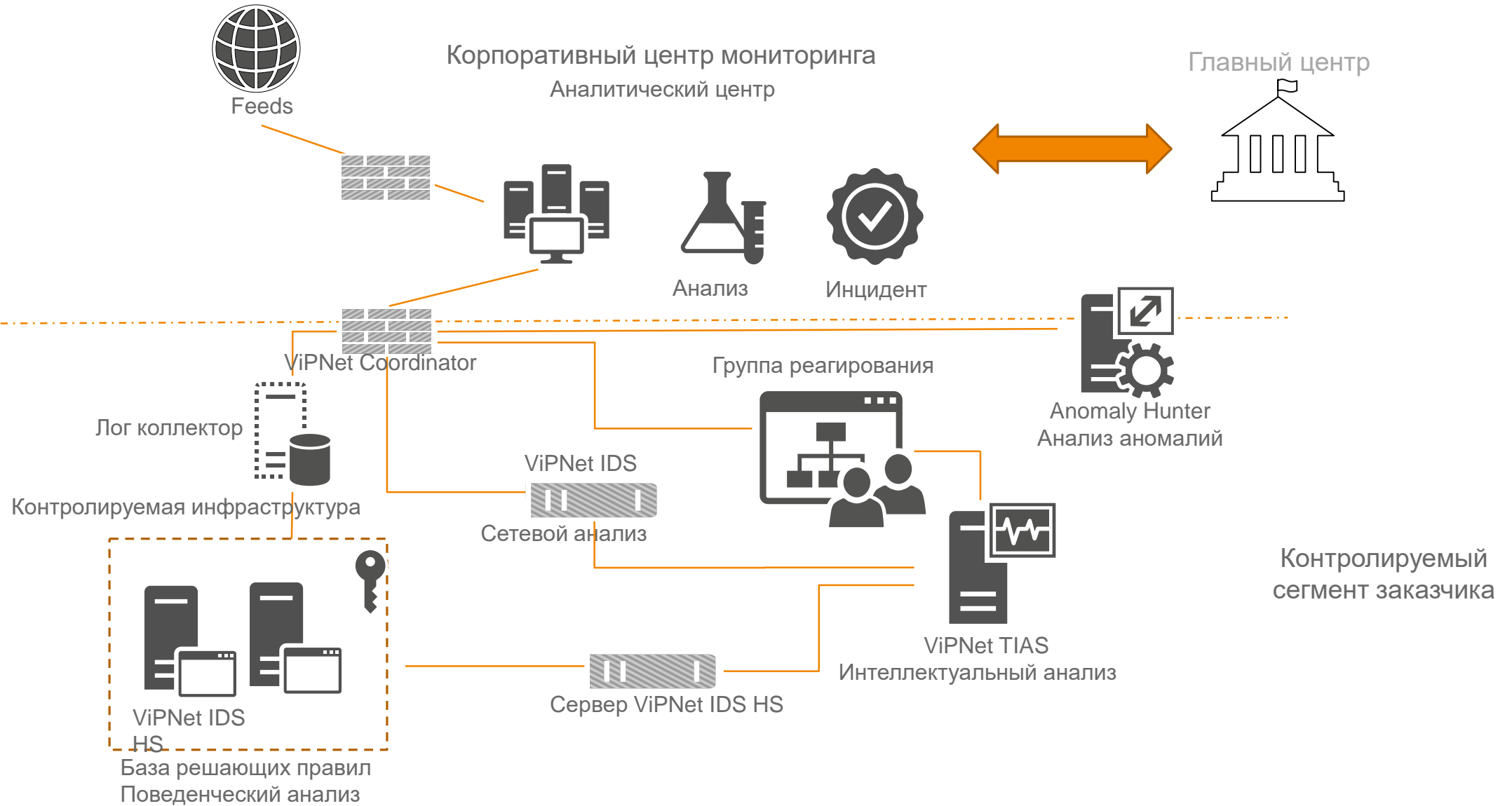
Список продуктов (2)

#	Важность	Имя	В Работе	Обратная Связь	Решена	Закрыта	Всего	Score ?
19	низкая	Linux Server 1	1	0	0	0	3	20
13	низкая	APM Windows msk-w0423	0	0	0	0	3	29

Обнаружение КА и инцидентов



Анализ событий и обнаружение КА



Управление и обработка инцидентов



⚠️ Успешная эксплуатация уязвимости в SMB (MS-17-010)

Критичность: Система: Главный ЦОД Обновлено: 8 days ago Investigate ▾

Метаправила: События: Создан: 07.05.2018 15:05

Детали Сопка

Маркер: Необходимо содействие

Дата создания: 07.05.2018 15:05

Дата фиксации: 07.05.2018 15:05

Дата изменения: 07.05.2018 15:05

Действия

User	2018-05-15T08:28:10.618000Z
Переустановлена операционная система	
Установлены последние обновления	

Рекомендации

User	2018-05-15T08:27:02.164000Z
Отключить пораженный компьютер от сети	
Осуществить антивирусную проверку	
Провести анализ сетевой активности узла	

Сигнатуры

ID	Название	Источник	События
30254125	AM Exploit SMB MS-17-0...	10.0.24.201	

События Ревизия **Комментарии 1** Активы Влияние Файлы Контакты

2 minutes ago
В системе обнаружен вирус-шифровальщик. Зашифрованные данные имели бэкапы дневной давности.

Новый комментарий

Выводы



Ресурсы



Корпоративный
центр ПМ

- ✓ Выявление КА и КИ
- ✓ Реагирование
- ✓ Разработка правил
- ✓ Выявление уязвимостей
- ✓ Адаптация новых источников данных
- ✓ Экспертная поддержка
- ✓ Сбор и передача сведений в НКЦКИ

Техническое обеспечение

- ✓ Средства сбора и анализа событий
- ✓ Средства выявления аномалий
- ✓ Система управления уязвимостями
- ✓ Система управления инцидентами
- ✓ Отправка сведений в НКЦКИ



Спасибо за
внимание!

И подключайтесь к
ГосСОПКА

Роман Кобцев

Директор по развитию бизнеса
компании «Перспективный мониторинг»

Roman.Kobtsev@amonitoring.ru