ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

Организационные и технические вопросы подключения к ГосСОПКА.

Роман Кобцев, директор по развитию бизнеса

ЗАО «Перспективный мониторинг», ГК «ИнфоТеКС»

disclaimer

Регулирование безопасности КИИ сейчас находится в фазе активной подготовки нормативных и правовых актов. Презентация является лишь экспертным мнением, основанном на изучении существующих документов и личном опыте, и не может быть использована как руководство. Для получения достоверной и полной информации о подключении своих организаций к ГосСОПКА направляйте соответствующий запрос в Национальный координационный центр по компьютерным инцидентам (НКЦКИ) или другие подразделения ФСБ России, отвечающие за координацию в данной сфере.

Национальный координационный центр по компьютерным инцидентам (НКЦКИ) готов принимать вопросы и предложения, связанные с функционированием ведомственных и корпоративных центров с НКЦКИ.
Вопросы направляйте на электронную почту:

gs@gov-cert.ru

План выступления

В выступлении будут затронуты только основные организационные вопросы.

Некоторые вопросы затрагивать преждевременно.

Говорить о гостайне в КИИ и ГосСОПКА преждевременно

Федеральный закон от 26.07.2017 N 193-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"

УКАЗ Президента России
от 2 марта 2018 г. N 98 О внесении изменения в перечень сведений, отнесенных к государственной тайне, утвержденный указом президента российской федерации от 30 ноября 1995 г. N 1203

Ждем расширенные перечни

СОПКА

ГосСОПКА

Основание подключения к ГосСОПКА

Федеральный закон от 26.07.2017 N 187-ФЗ

"О безопасности критической информационной инфраструктуры Российской Федерации"

Указ Президента РФ от 15 января 2013 г. N 31с

«О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

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)

Указ Президента РФ от 15 января 2013 г. N 31с

«О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

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**)

Документы будут действовать до введения требований к корпоративным и ведомственным центрам ГосСОПКА или другим НПА их заменяющих

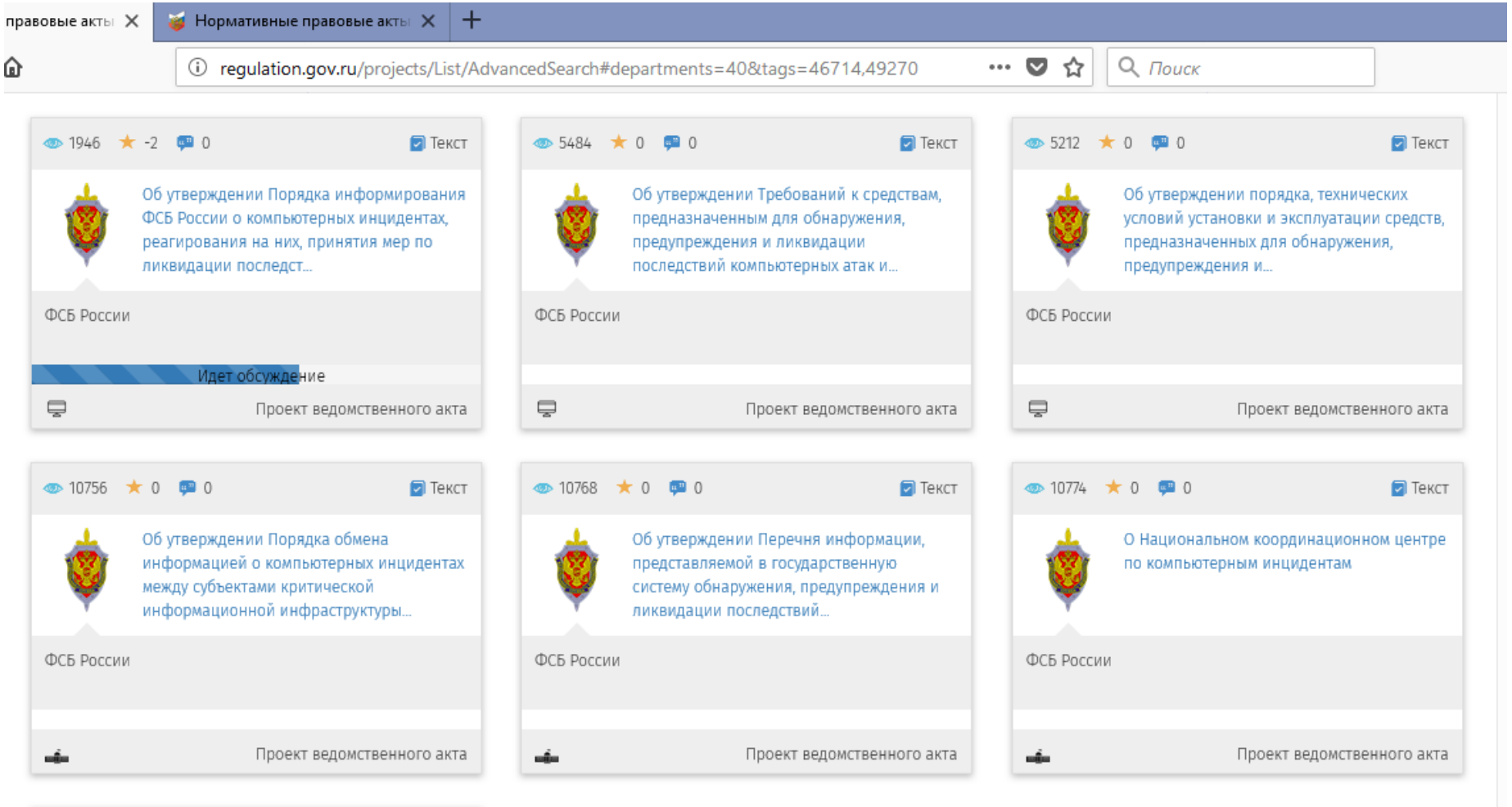
Методические рекомендации ФСБ России по созданию ведомственных сегментов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Временный порядок включения корпоративных центров в ГосСОПКА

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

Опубликованы проекты



Опубликованы проекты

- Проект приказа ФСБ России «О Национальном координационном центре по компьютерным инцидентам (НКЦКИ)»
- Проект приказа ФСБ России «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»
- Проект приказа ФСБ России «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»

Опубликованы 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»

Ожидаем проекты

- Проект приказа ФСБ России «Положение о ГосСОПКА»
- Проект приказа ФСБ России «Требования к ведомственным (корпоративным) центрам ГосСОПКА»

Федеральный закон от 26.07.2017 N 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, Финцерт ЦБ РФ для финансовых организаций), а также реагировать на компьютерные инциденты в установленном порядке.

Перечень сведений, представляемых в ГосСОПКА

Все подробности взаимодействия прописаны в п.8 Методических рекомендаций ФСБ России по созданию ведомственных сегментов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

- информацию о зоне ответственности сегмента ГосСОПКА;
- данные об информационных ресурсах;
- данные о компьютерных атаках;
- данные о компьютерных инцидентах;
- общую информацию о защищенности информационных ресурсов;
- детальную информацию о защищенности информационных ресурсов, доступных из сети Интернет;
- статистические данные об актуальных для сегмента ГосСОПКА угрозах;
- сведения о самостоятельно обнаруженных индикаторах компрометации информационных ресурсов.


Создание вед. сегмента
Подключение к корп. сегменту
Гибридная модель

В соответствии с методическими рекомендациями ФСБ, выполнение данного требования закона возможно следующими способами:

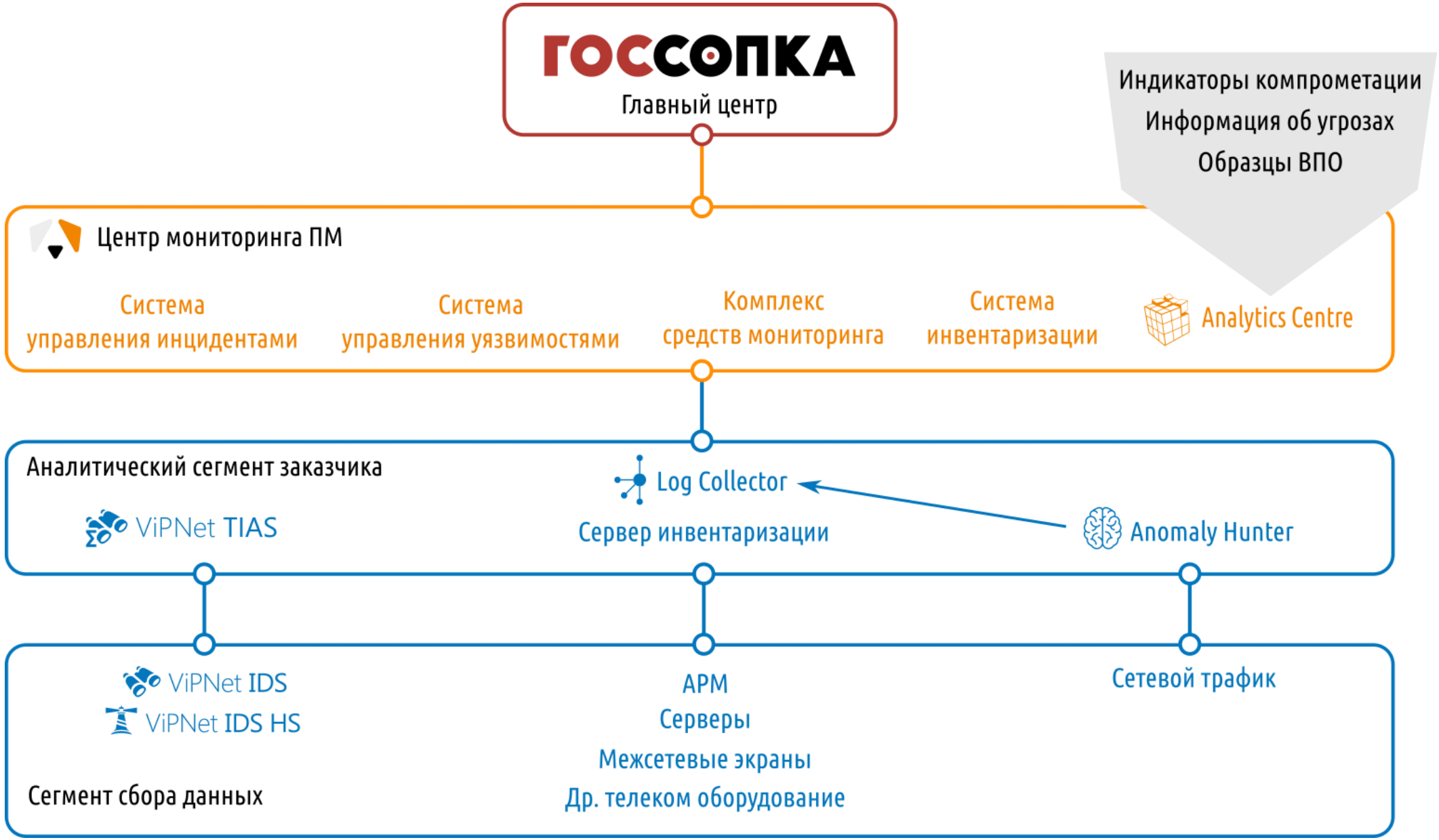

Источники угроз
Атакованные системы
Сведения об инфраструктуре
Компьютерные инциденты
Уязвимости
Состояние защищённости
Индикаторы компрометации
ГОССОПКА
НКЦКИ
Головной центр ГосСОПКА
Центр ГосСОПКА
Центр ГосСОПКА
Головной центр ГосСОПКА
Ведомственные центры
Корпоративные центры
Подчинённый центр
Подчинённый центр
Подчинённый центр
Подчинённый центр
Сегмент ГосСОПКА

В случае создания собственного корпоративного сегмента:

- ✓ Заключить соглашение с 8Ц ФСБ России на создание корпоративного сегмента
- ✓ Выполнить организационные и технические требования в соответствии с методическими рекомендациями
- ✓ Развернуть специализированные системы взаимодействия сегмента ГосСОПКА с главным (или территориальным) центром ГосСОПКА

Неочевидный нюанс:

Нужно ли ведомственному (корпоративному) центру ГосСОПКА получать лицензию ФСТЭК России на деятельность по мониторингу ИБ в рамках ТЗКИ если у него в иерархии есть подчиненные центры?


ГОССОПКА
Главный центр
Индикаторы компрометации
Информация об угрозах
Образцы ВПО
Центр мониторинга ПМ
Система управления инцидентами
Система управления уязвимостями
Комплекс средств мониторинга
Система инвентаризации
Analytics Centre
Аналитический сегмент заказчика
ViPNet TIAS
Log Collector
Сервер инвентаризации
Anomaly Hunter
ViPNet IDS
ViPNet IDS HS
Сегмент сбора данных
АРМ
Серверы
Межсетевые экраны
Др. телеком оборудование
Сетевой трафик

В соответствии с п. 2.2.7 методическими рекомендации ФСБ России:

Организация, принявшая решение о создании сегмента ГосСОПКА, может поручить выполнение отдельных функций, определенных в разделе 3 настоящих методических рекомендаций, организациям, осуществляющим лицензируемую деятельность в области защиты информации.

В случае подключения через сторонний корпоративный сегмент:

- ✓ Заключить соглашение с корпоративным центром
- ✓ Уведомить Главный центр ГосСОПКА о включении своих информационных ресурсов в зону ответственности корпоративного центра.

Уведомляя Главный центр ГосСОПКА субъект КИИ указывает:

- ✓ перечень всех своих информационных систем;
- ✓ перечень информационных систем, включаемых в зону ответственности корпоративного центра;
- ✓ номер договора и срок его действия (в случае отсутствия номера договора указывается намерение по его заключению и предполагаемый срок его действия).

Корпоративный центр информирует Главный центр ГосСОПКА о включении информационных ресурсов Объекта КИИ в зону своей ответственности. При этом указывает:

- ✓ перечень информационных систем Объекта КИИ, включаемых в зону ответственности;
- ✓ номер договора и срок его действия;
- ✓ инвентаризационную информацию об ИС Объекта КИИ в течении трех месяцев с момента включения ИС Объекта КИИ в зону его ответственности.

Спасибо за внимание!

Роман Кобцев

Директор по развитию бизнеса

компании «Перспективный мониторинг»

Roman.Kobtsev@amonitoring.ru