

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Подключение к ГосСОПКА. Оргвопросы

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.

Выступления представителей регулятора доступны в интернете



https://soc-forum.ib-bank.ru/materials2017

IB-BANK.RU
ОТРАСЛЕВОЙ ПОРТАЛ

МЕРОПРИЯТИЯ ЖУРНАЛ ТВ ОБРАЗОВАНИЕ КАТАЛОГ ИЗДАТЕЛЬСТВО СЛОВАРЬ

Фотоотчет 2017
SOC-Форум СТГ
Пост-релиз
Программа
Партнеры
Подписка
SOC-Форум 2016
Контакты

Сессия 1

Функционирование и взаимодействие центров ГосСОПКА. Вопросы регулирования деятельности SOC

О нормативном регулировании деятельности центров ГосСОПКА
Андрей Раевский, сотрудник ФСБ России [Скачать](#)

Роль центров ГосСОПКА в обеспечении безопасности критической информационной инфраструктуры Российской Федерации
Анатолий Грачев, сотрудник ФСБ России [Скачать](#)

Введите запрос

Введите запрос

2:00 / 11:50

23:01 / 28:04

YouTube

Введите запрос

BIS TV

5:50 / 13:49



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



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**)



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

Опубликованы проекты

правовые акты X Нормативные правовые акты X +

regulation.gov.ru/projects/List/AdvancedSearch#departments=40&tags=46714,49270 Поиск

1946 -2 0 Текст


 Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последст...

ФСБ России

Идет обсуждение

Проект ведомственного акта


5484 0 0 Текст

 Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и...

ФСБ России

Проект ведомственного акта


5212 0 0 Текст

 Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и...

ФСБ России

Проект ведомственного акта


10756 0 0 Текст

 Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры...

ФСБ России

Проект ведомственного акта


10768 0 0 Текст

 Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий...

ФСБ России

Проект ведомственного акта

10774 0 0 Текст

 О Национальном координационном центре по компьютерным инцидентам

ФСБ России

Проект ведомственного акта

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»

Ждем проекты

- Проект приказа ФСБ России «Положение о ГосСОПКА»
- Проект приказа ФСБ России «Методические рекомендации по проведению мероприятий по оценке степени защищенности, обнаружению компьютерных атак, предупреждению и ликвидации последствий КИ»
- Проект приказа ФСБ России «Методические рекомендации по проведению мероприятий по ликвидации последствий КИ»
- Проект приказа ФСБ России «Методические рекомендации по обнаружению компьютерных атак»
- 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.



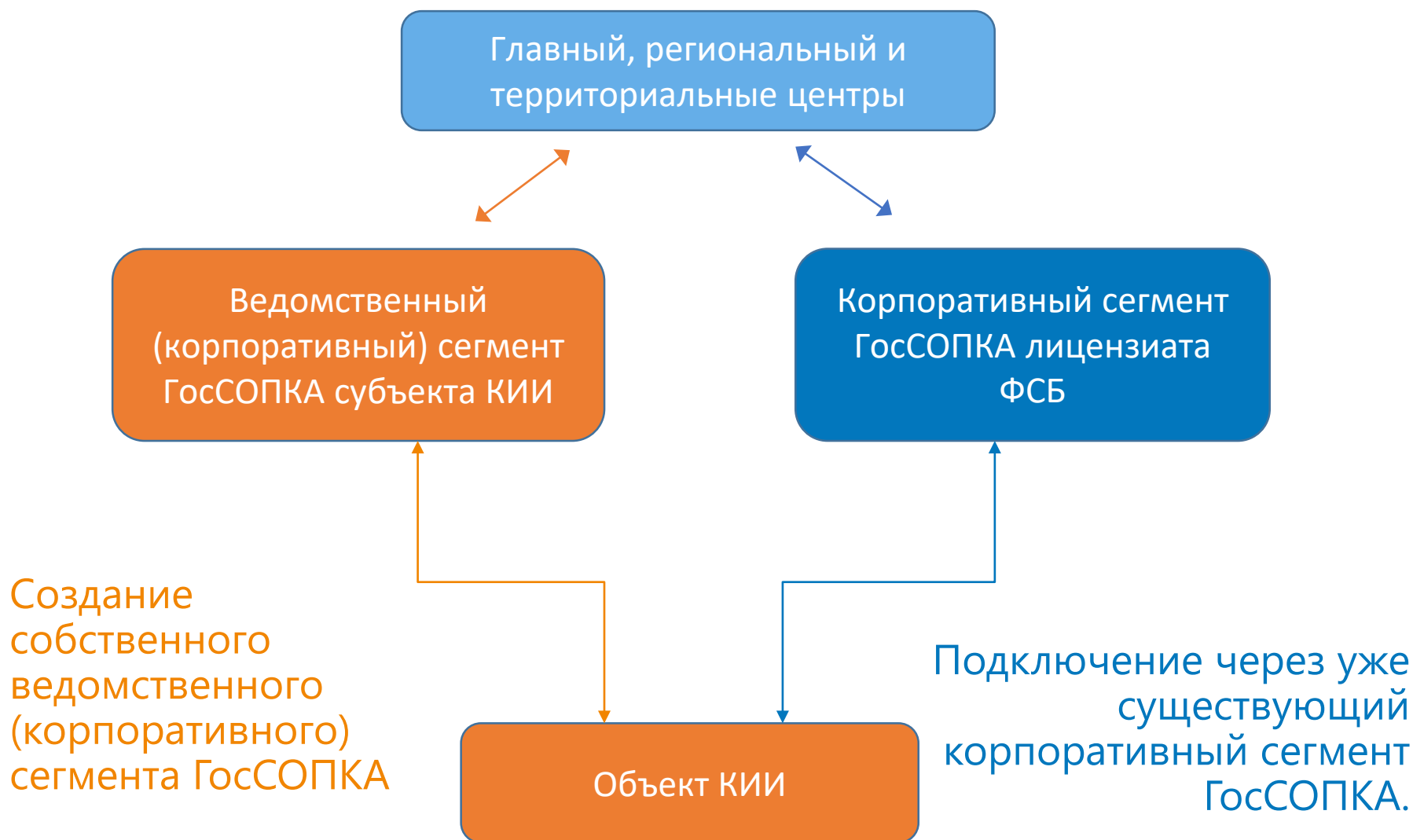
Перечень сведений, представляемых в ГосСОПКА

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.



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



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



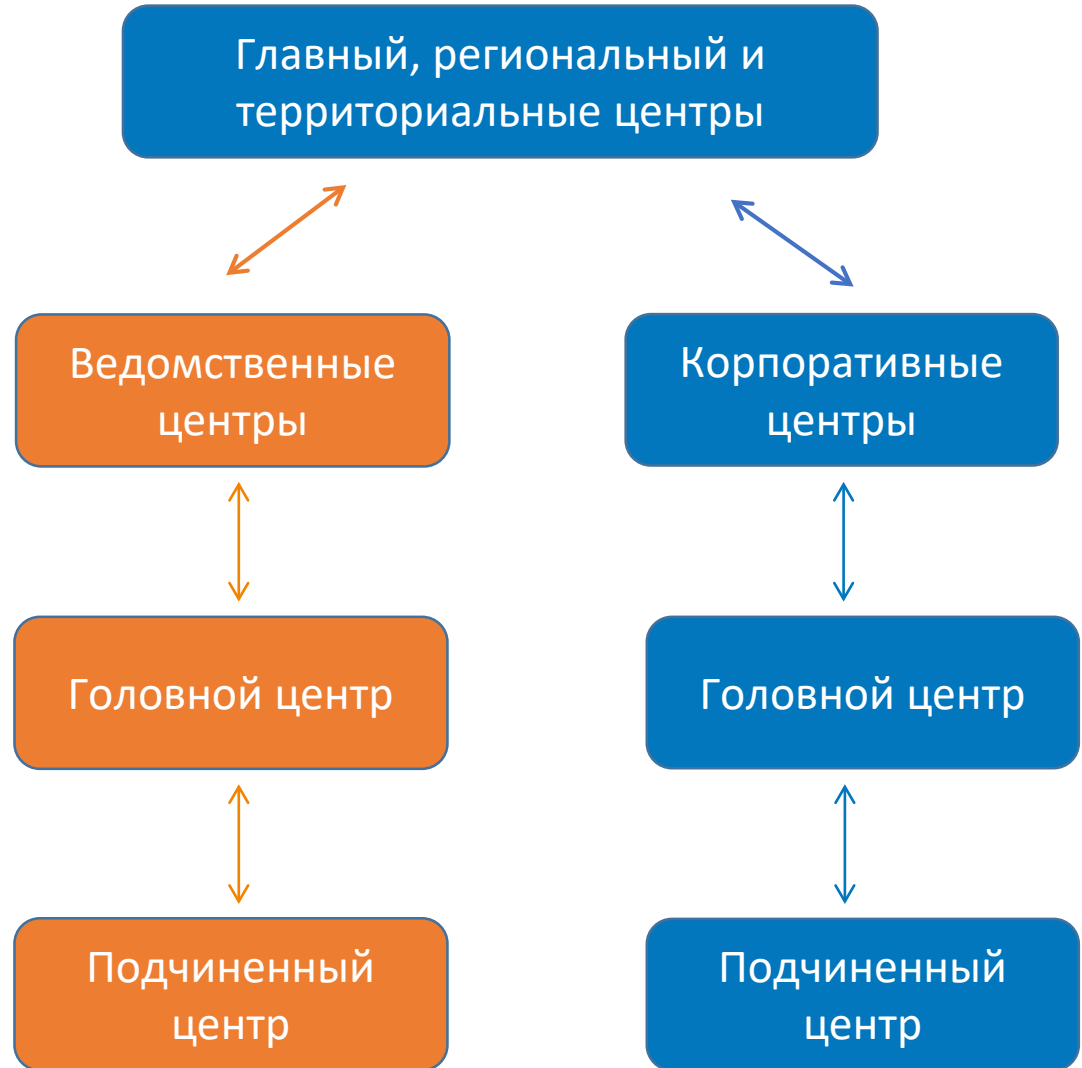
В соответствии с методическими рекомендациями ФСБ России:

Головной центр
ГосСОПКА —

наивысшая структура в иерархии центров, объединенных по ведомственному или организационному признакам.

Подчиненный центр
ГосСОПКА —

центр ГосСОПКА, имеющий структурное подчинение головному центру 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?





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