Взаимодействие объектов критической информационной инфраструктуры с ГосСОПКА. Возможные схемы и неочевидные нюансы

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.

План выступления

Взаимодействие объектов КИИ с ГосСОПКА тема очень обширная, и охватить ее в одной презентации не возможно. Поэтому в выступлении будут затронуты только основные организационные вопросы.

Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"


Она не одна придет.. Она с кузнецом придет

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"

Федеральный закон от 26.07.2017 N 194-ФЗ

"О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации»

Согласно Федеральному закону от 26.07.2017 №193-ФЗ

"О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"

Положения Федерального закона от 26.12.2008 N 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля, устанавливающие порядок организации и проведения проверок, не применяются также при осуществлении государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

Согласно Федеральному закону от 26.07.2017 №193-ФЗ

"О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"

Вносятся изменения в Закон Российской Федерации от 21 июля 1993 года N 5485-1 «О государственной тайне», согласно которым сведения о мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак составляют государственную тайну

Согласно Федеральному закону от 26.07.2017 №193-ФЗ

"О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"

Вносятся изменения в Федеральный закон от 7 июля 2003 года N 126-ФЗ «О связи» накладывающие дополнительные обязанности на операторов связи по соблюдению порядка, технических условий установки, эксплуатации и сохранности средств, предназначенных для поиска признаков компьютерных атак.

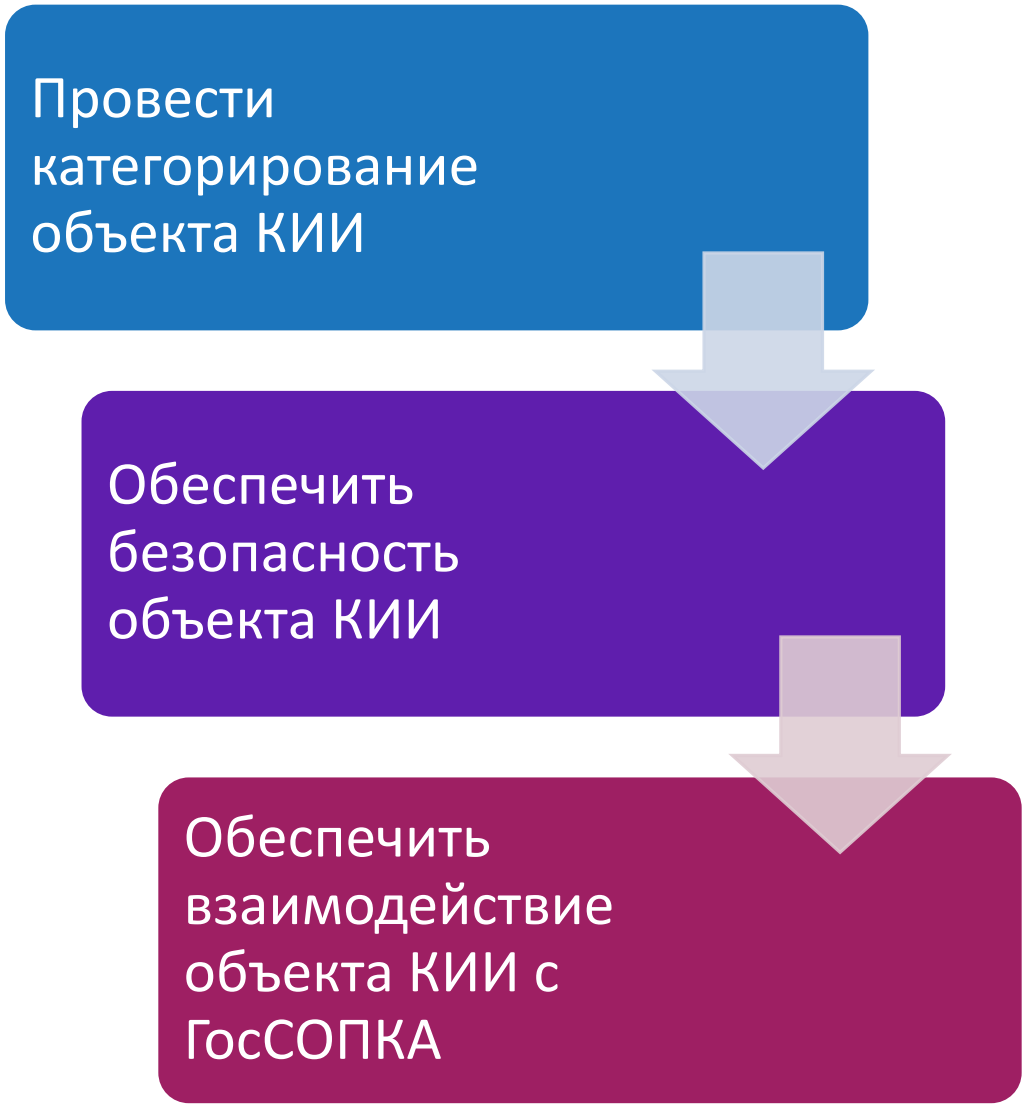
Согласно Федеральному закону от 26.07.2017 №194-ФЗ

"О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации»

В УК РФ вводится Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

С максимальным сроком до 10 лет лишения свободы (в т. ч. за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации в КИИ)

Федеральный закон от 26.07.2017 N 187-ФЗ обязывает субъекта КИИ



Закон вступает в силу 1 января

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**)


Главный, региональный и территориальные центры
Создаёт и эксплуатирует ФСБ
Ведомственные центры
Орган государственной власти или лицензиат
Корпоративные центры
Госкорпорация, оператор связи или лицензиат

Методические рекомендации ФСБ России по созданию ведомственных сегментов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации *Утверждены в декабре 2016 г.*

Федеральный закон от 26.07.2017 N 187-ФЗ

Ч.4 ст11 Перечень сведений, представляемых в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и порядок их представления устанавливает федеральный орган исполнительной власти, уполномоченный в области создания и обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Субъект критической информационной инфраструктуры обязан информировать в порядке, установленном федеральным органом исполнительной власти, уполномоченным в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и обеспечения ее функционирования, о компьютерных инцидентах.

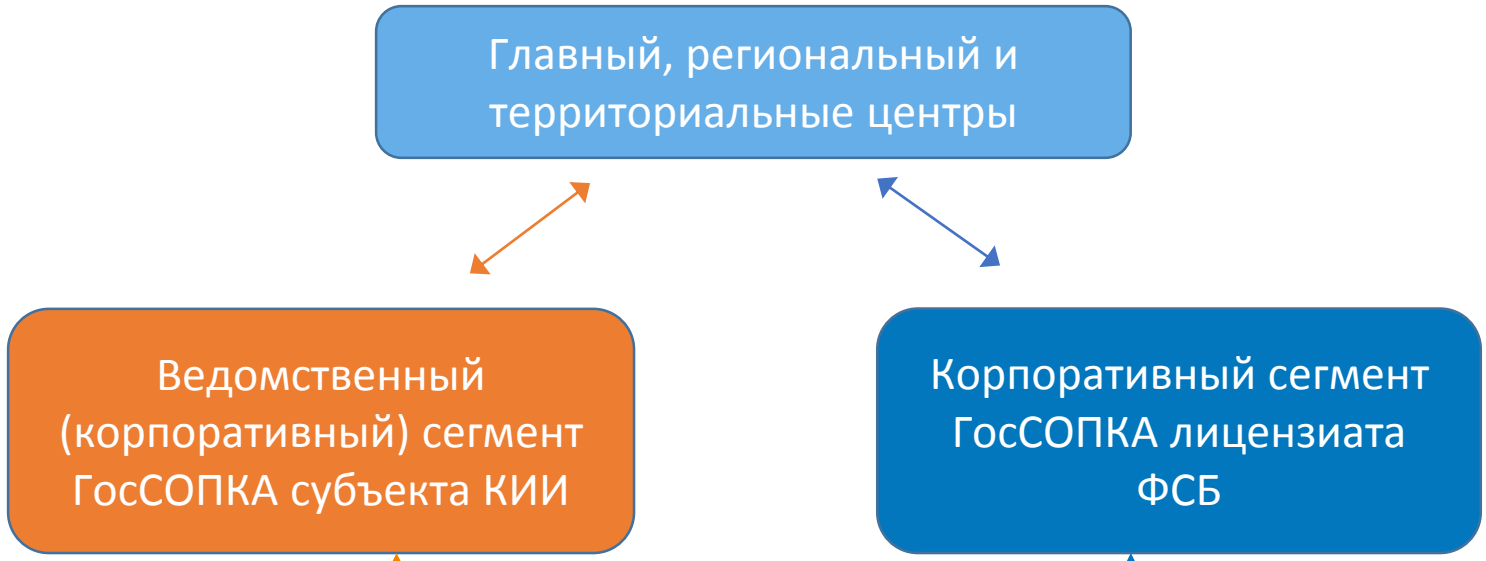
Перечень сведений, представляемых в ГосСОПКА

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:



Создание собственного ведомственного (корпоративного) сегмента ГосСОПКА

Объект КИИ

Подключение через уже существующий корпоративный сегмент ГосСОПКА.

Возможны все варианты

Но есть нюансы в стратегии

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

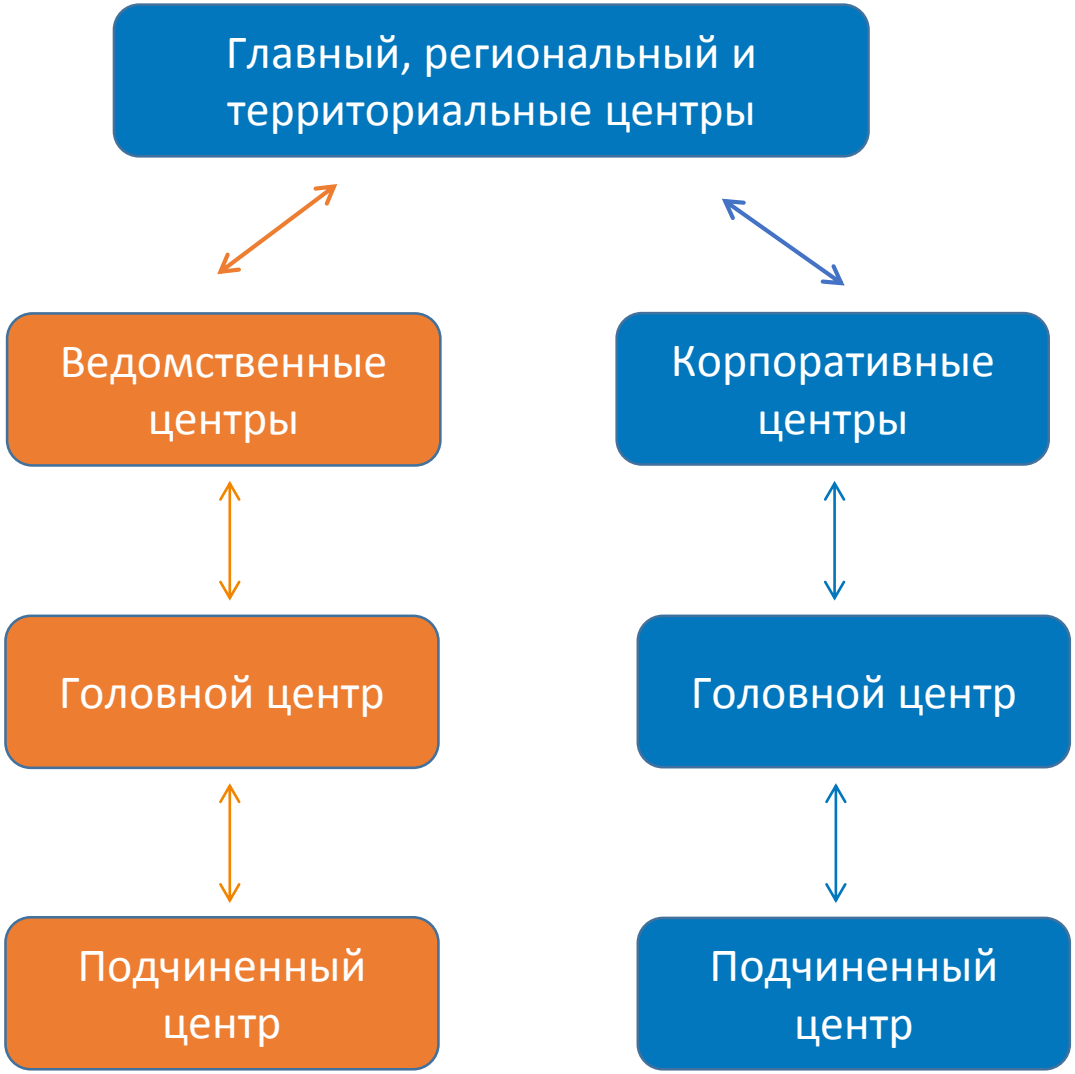
В соответствии с методическими рекомендации ФСБ России:

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?

Субъективное мнение:

Скорее всего ВЦ (КЦ) ГосСОПКА лицензия ТЗКИ не потребуется, если не происходит оказания платных услуг.

Точный ответ:

Необходимо направить запрос в ФСТЭК России, в котором описать организацию, ее деятельность, цели и задачи в интересах которых планируется осуществлять мониторинг ИБ, и запросить, подпадает ли эта деятельность под лицензируемые виды деятельности.

Неочевидный нюанс:

В методических рекомендациях есть раздел «Рекомендации по кадровому обеспечению». Однако требования к персоналу корпоративного центра прописаны во временном регламенте включения корпоративных центров в состав ГосСОПКА, и они достаточно жесткие.

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.

Неочевидный нюанс:

Наличие уже установленных средств региональных центров ГосСОПКА не отменяет необходимости субъекту КИИ создавать корпоративный (ведомственный) центр и выполнять требования методических рекомендаций.

Неочевидный нюанс:

Создание субъектом КИИ корпоративного (ведомственного) центра не отменяет уже установленных средств региональных центров ГосСОПКА. Средства региональных центров ГосСОПКА во всех случаях продолжают функционировать.

В настоящее время ведется разработка нормативных и правовых актов, регулирующих вопросы взаимодействия с ГосСОПКА. До конца года ожидаются положение по ведомственным и корпоративным центрам ГосСОПКА и регламент их взаимодействия с НКЦКИ.

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

Спасибо за внимание!

Роман Кобцев

Директор по развитию бизнеса

компании «Перспективный мониторинг»

Roman.Kobtsev@amonitoring.ru