



ПЕРСПЕКТИВНЫЙ  
МОНИТОРИНГ

# Опыт центра ГосСОПКА

Роман Кобцев

Директор по развитию бизнеса ЗАО «Перспективный мониторинг»

---



# Корпоративный Центр ГосСОПКА с 2017 года

<...>

И мы с вторых печатаем портреты,  
Хоть в этом, право, и не их вина,  
Они - наш флаг, и дети всей планеты  
Проходят в школах эти имена.

Но я прошу, чтоб мы на этом свете,  
Собравшись вместе, хоть когда-нибудь,  
Не позабыли, славя первых этих,  
Всех настоящих первых помянуть.

А, Макаревич



# Центр мониторинга ЗАО «ПМ»



Год запуска — 2014

Соглашение с ФСБ России

Лицензия ФСТЭК России  
на мониторинг ИБ

Более 30 операторов,  
исследователей,  
аналитиков и инженеров

Более 20 клиентов

7 200 собственных  
сигнатур атак для IDS

388 млн событий за 11  
месяцев 2018 года

Более 1000 инцидентов за  
11 месяцев 2018 года

<60 мин. — реагирование  
на инцидент ИБ



# Организационная часть



# КИИ или НЕ КИИ?

Мы еще не направляли документы во ФСТЭК, но провели работы по категорированию своего центра мониторинга как объекта КИИ.





# Государственная тайна

На сегодня у нас не было опыта взаимодействия с объектами ГосСОПКА, обрабатывающих сведения, составляющие гостайну.

Этот вопрос по многим параметрам еще пока остается открытым.





Комплект нормативных  
правовых актов по вопросам  
взаимодействия с ГосСОПКА  
пока не полный, но работать  
есть с чем.



# 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.



- **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.



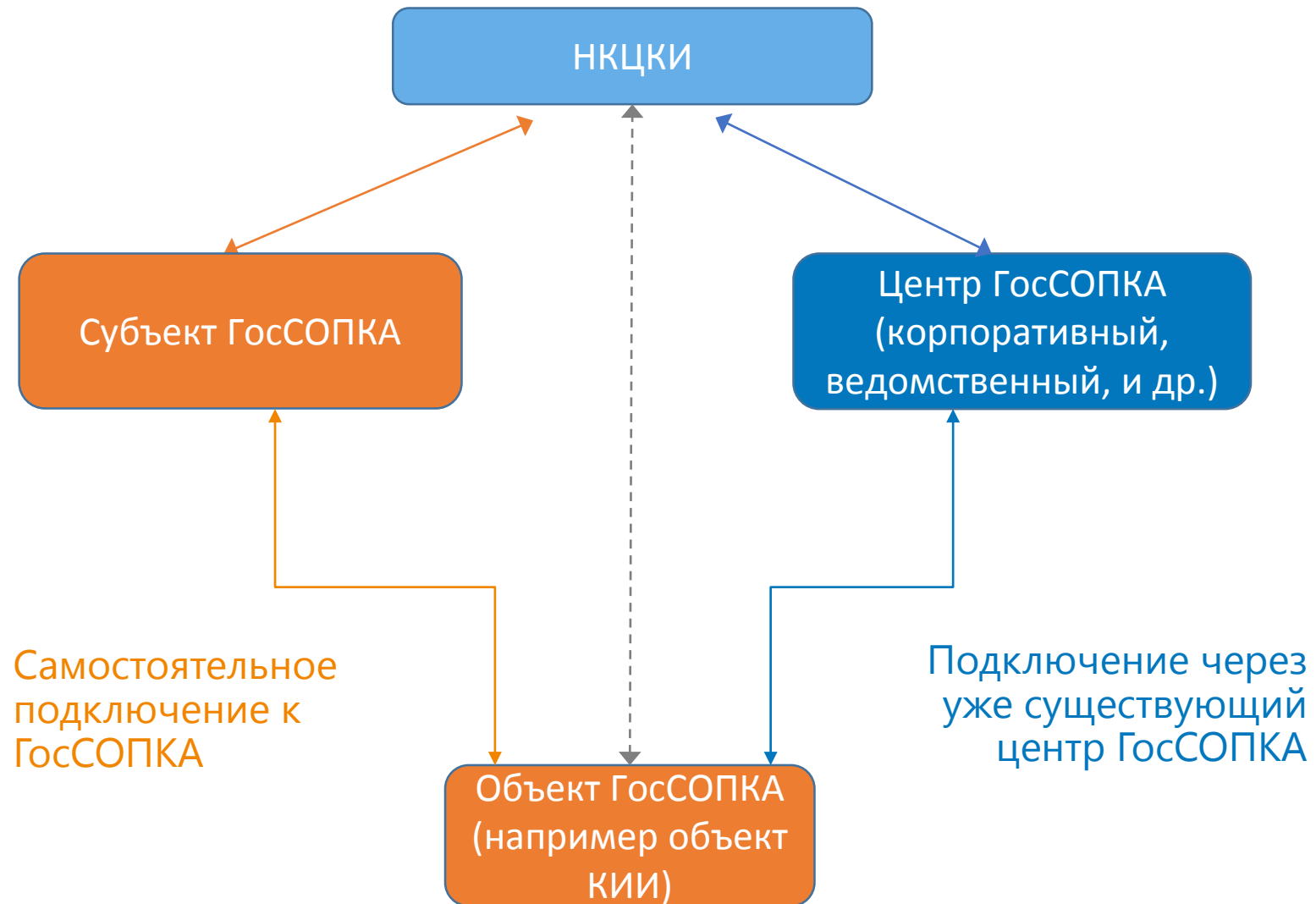
- Методические рекомендации ФСБ России по созданию ведомственных сегментов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
- Методические рекомендации ФСБ России по обнаружению компьютерных атак на информационные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

# Документы НКЦКИ дают большую свободу в выстраивании иерархического взаимодействия с ГосСОПКА



Главное, четко разграничить, кто в этой иерархии за какие функции отвечает





# 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.

# Два способа предоставления информации в НКЦКИ:



С использованием  
технической  
инфраструктуры НКЦКИ



Посредством электронной,  
факсимильной, почтовой и  
телефонной связи.

**Автоматизированное взаимодействие с технической инфраструктурой НКЦКИ сильно сэкономит ваши силы и время**



# Взаимодействие с технической инфраструктурой НКЦКИ



Портал   Информация   Расследование

Инциденты Добавить

Найденные инциденты

ID	Название	Критичность	Система	Пораженные активы	Тип	Статус	Состояние	Время фикса
5b9275bc232fba000ec1085c	Множественные попытки доступа по RDP к узлу контр...	high	971fe2b4-3fb6-4f9b-af82-d558...		brute_forces	новый	предполагаемый	07.09.2018 15:57
5b7d9010232fba000c20855e	sdfsdfsdf	high	971fe2b4-3fb6-4f9b-af82-d558...		traffic_hijac...	новый	предполагаемый	22.08.2018 19:32
5b7d8fc7232fba000c20855c	fddfgdfg		971fe2b4-3fb6-4f9b-af82-d558...			новый	предполагаемый	22.08.2018 19:31
5b7d8d8f232fba0017971b6f	ssdfsdf	high	971fe2b4-3fb6-4f9b-af82-d558...		traffic_hijac...	новый	предполагаемый	22.08.2018 19:21
5b7ae68e232fba000eb009e8	вапвап	high	971fe2b4-3fb6-4f9b-af82-d558...		traffic_hijac...	новый	предполагаемый	20.08.2018 19:04
5b6c3c58232fba000c208551			971fe2b4-3fb6-4f9b-af82-d558...			новый	предполагаемый	09.08.2018 16:06
5b6adb9232fba000b94edb9	bbb		971fe2b4-3fb6-4f9b-af82-d558...			новый	предполагаемый	08.08.2018 15:02
5b6ad9f1232fba000b94edb7	sdfsdf		971fe2b4-3fb6-4f9b-af82-d558...			новый	предполагаемый	08.08.2018 14:54
5b6ad8ac232fba000eb009e5	aaa		971fe2b4-3fb6-4f9b-af82-d558...			новый	предполагаемый	08.08.2018 14:49
5b6ad4ad232fba000b94edae			971fe2b4-3fb6-4f9b-af82-d558...	10.91.142.28		новый	предполагаемый	08.08.2018 14:31

Выводить по 20 |< < 1/1 > >| Всего: 10

# Взаимодействие с технической инфраструктурой НКЦКИ



Портал Информация Расследование

Инциденты / 5b9275bc232fba000ec1085c Синхронизировать с НКЦКИ Редактировать

## ⚠ Множественные попытки доступа по RDP к узлу контролируемой сети

**Критичность:** high      **Система:** 971fe2b4-3fb6-4f9b-af82-d55837207f84      **Дата фиксации:** 07.09.2018 15:57      **Дата создания:** 07.09.2018 15:57      **Дата изменения:** 07.09.2018 16:05

**Состояние:** предполагаемый      **Статус:** новый      **Пользователь:**      **Метаправила:**  Необходимо содействие НКЦКИ

**Тип:** brute\_forces      **Ограничительный маркер:**      **Количество событий:**

**Описание инцидента:**  
Выявлены многочисленные попытки подбора пароля для доступа по RDP к узлу контролируемой сети

**Рекомендации**

- 1. Отключить пораженный актив от вычислительной сети
- 2. Провести интервьюирование владельца
- 3. Заблокировать на межсетевом экране IP-адрес атакующего
- 4. Провести аудит открытых портов и запущенных служб и закрыть неиспользуемые
- 5. Настроить ограничение количества неуспешных попыток доступа в систему
- 6. Ограничить доступ списком доверенных IP-адресов

Установить пароли надлежащей сложности для доступа к узлу

**Действия**

- Сформирован белый список доступа
- Заблокирован IP адрес атакующего на МСЭ

События История Комментарии Пораженные активы **Влияние** Файлы Контакты

brute\_forces 1

brute\_force-0

id: 122334

Цель

IP: 125.54.12.354      URL:      Тип сетевого сервиса: RDP

Источники

ip

15.55.21.14

15.25.55.14



Спасибо за  
внимание!

И подключайтесь к ГосСОПКА

## Роман Кобцев

Директор по развитию бизнеса  
компании «Перспективный мониторинг»

[Roman.Kobtsev@amonitoring.ru](mailto:Roman.Kobtsev@amonitoring.ru)