POSITIVE TECHNOLOGIES

Сергей Куц
направление по безопасности КИИ
skuts@ptsecurity.com

Взаимодействие КИИ и ГосСОПКА

Структура вебинара

Эволюция нормативной базы по ГосСОПКА

Центры ГосСОПКА: кто может строить, условия для создания и нормативная база

Порядок выполнения требований по ГосСОПКА для субъектов ГосСОПКА

POSITIVE TECHNOLOGIES

Обзор нормативной и методической базы по ГосСОПКА

POSITIVE TECHNOLOGIES

2012: основные направления госполитики

С чего все началось …

2009

Указ Президента РФ
от 12.05.2009 № 537
«О Стратегии национальной безопасности РФ до 2020 года»

уже утратил силу

2012

«Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры РФ»

Утверждены Президентом РФ 3.02.2012 г., № 803

Появляются термины:

- критическая информационная инфраструктура РФ
- единая государственная система обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру

POSITIVE TECHNOLOGIES

2013: Указ Президента

Указ Президента от 15 января 2013 г. № 31с

POSITIVE TECHNOLOGIES

2014: Концепция ГосСОПКА

Концепция ГосСОПКА № К 1274: терминология

Основное назначение ГосСОПКА:

обеспечение защищенности от компьютерных атак и штатного функционирования информационных ресурсов РФ при их возникновении

Силы ГосСОПКА

Средства ГосСОПКА

Субъекты ГосСОПКА

Концепция ГосСОПКА № К 1274: виды центров

ФСБ России

- Главный центр ГосСОПКА
- Региональный центр ГосСОПКА
- Территориальный центр ГосСОПКА
- Национальный координационный центр по компьютерным инцидентам (НКЦКИ)

Органы гос.власти

Ведомственный центр ГосСОПКА

Организации

Корпоративный центр ГосСОПКА

POSITIVE TECHNOLOGIES

2016: методические рекомендации ФСБ России

Методические рекомендации ФСБ России

Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации от 27.12.2016

Технические средства для выполнения функций ГосСОПКА

1. Средства взаимодействия персонала
2. Средства взаимодействия с НКЦКИ ГосСОПКА
3. Средства инвентаризации информационных систем
4. Средства выявления уязвимостей
5. Средства анализа событий безопасности
6. Средства учета и обработки инцидентов

POSITIVE TECHNOLOGIES

2017: указ Президента № 620

Совершенствование ГосСОПКА

Указ Президента РФ от 22.12.2017 № 620

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

На чём в первую очередь необходимо сконцентрировать усилия. Первое – это совершенствование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России.

В. Путин
Заседание Совета Безопасности
Российской Федерации
26.10.2017 г.

Указ Президента №620 vs №31с: что изменилось

- Появилась ссылка на 187-ФЗ

- ФСБ России может контролировать защищенность не только КИИ, но в целом информационных ресурсы РФ от атак

- ФСБ России разрабатывает методические рекомендации:
  - по обнаружению компьютерных атак на информационные ресурсы РФ
  - по предупреждению и установлению причин компьютерных инцидентов, связанных с функционированием информационных ресурсов РФ, а также по ликвидации последствий этих инцидентов

POSITIVE TECHNOLOGIES

2018: вступил в силу 187-ФЗ

187-ФЗ о безопасности КИИ РФ от 26.07.2017

Установил права
и обязанности субъектов КИИ

ФСБ России наделен полномочиями
на уровне федерального закона

187-ФЗ о безопасности КИИ РФ от 26.07.2017

Установил права и обязанности субъектов КИИ

Задачи по защите значимых объектов КИИ:

- Защита от неправомерного доступа к информации, обрабатываемой КИИ
- Защита от негативных воздействий, в результате которых может быть нарушено и (или) прекращено функционирование объекта КИИ
- Восстановление функционирования объекта КИИ
- **Непрерывное взаимодействие с ГосСОПКА**

ФСБ России наделен полномочиями на уровне федерального закона

187-ФЗ о безопасности КИИ РФ от 26.07.2017

Установил права и обязанности субъектов КИИ

Задачи по защите значимых объектов КИИ:

- Защита от неправомерного доступа к информации, обрабатываемой КИИ
- Защита от негативных воздействий, в результате которых может быть нарушено и (или) прекращено функционирование объекта КИИ
- Восстановление функционирования объекта КИИ
- **Непрерывное взаимодействие с ГосСОПКА**

ФСБ России наделен полномочиями на уровне федерального закона

1. Создает Национальный координационный центр по компьютерным инцидентам
2. Координирует субъектов КИИ по реагированию на инциденты
3. Устанавливает порядок информирования об инцидентах, определяет состав предоставляемой информации
4. Устанавливает требования к средствам ГосСОПКА
5. Организует установку на объекты КИИ технических средств ГосСОПКА и устанавливает требования к ним
6. Организует и проводит оценку безопасности объектов КИИ

Приказы по ГосСОПКА

Приняты:

- **Приказ ФСБ России от 24.07.2018 № 366** о Национальном координационном центре по компьютерным инцидентам»
- **Приказ ФСБ России от 24.07.2018 № 367** об утверждении Перечня информации, представляемой в ГосСОПКА, и Порядка представления информации в ГосСОПКА
- **Приказ ФСБ России от 24.07.2018 № 368** об утверждении Порядка обмена информацией о компьютерных инцидентах

Проекты:

- **Приказ ФСБ России** об утверждении Требований к средствам ГосСОПКА
- **Приказ ФСБ России** об утверждении порядка, технических условий установки и эксплуатации средств ГосСОПКА
- **Приказ ФСБ России** об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак
- **Приказ Минкомсвязи России** об утверждении порядка, технических условий установки и эксплуатации средств для поиска признаков атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ

POSITIVE TECHNOLOGIES

Обзор приказов ФСБ России

Приказ ФСБ России № 366

Приказ ФСБ России от 24.07.2018 № 366 о Национальном координационном центре по компьютерным инцидентам

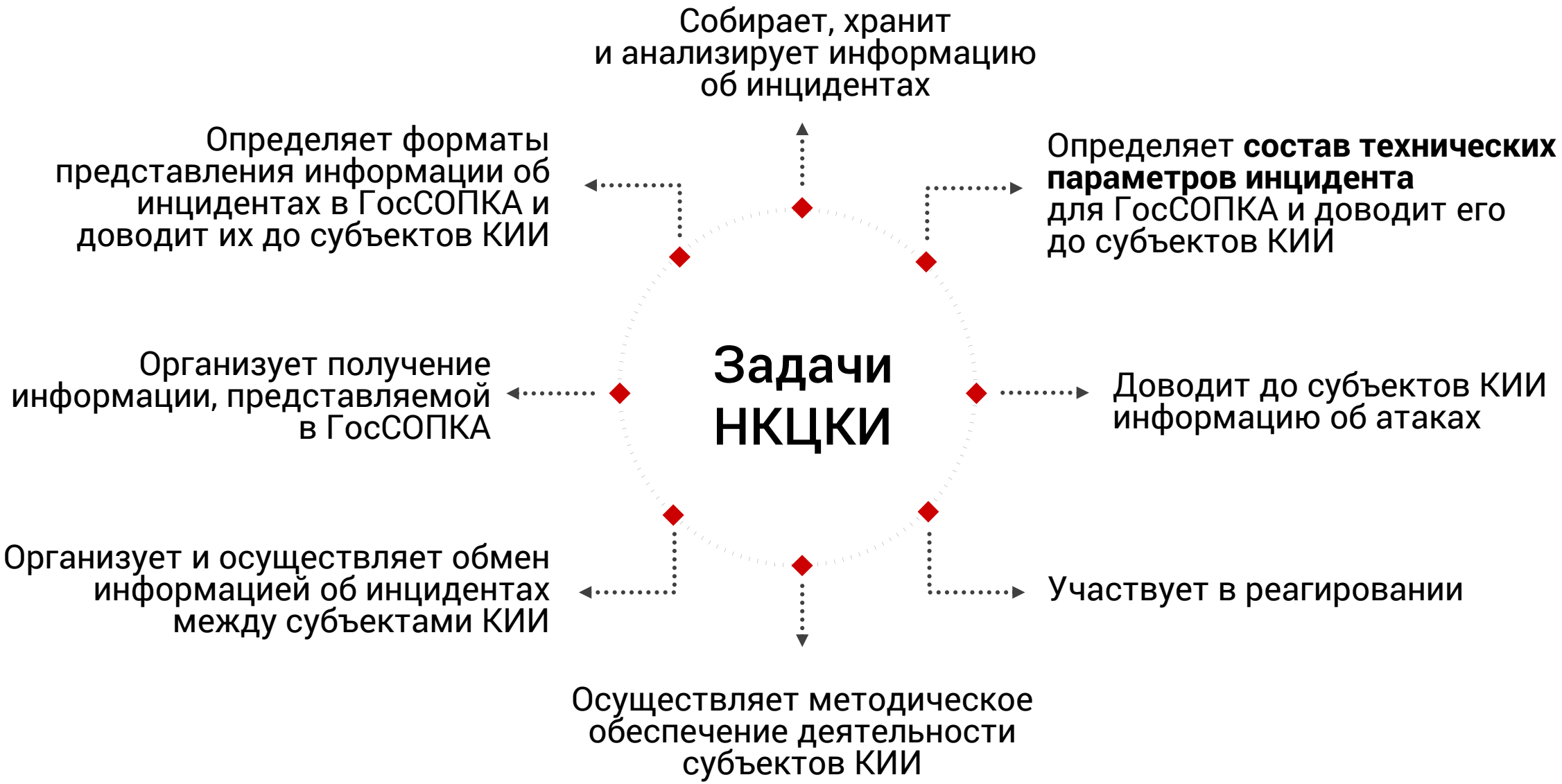
Задача НКЦКИ:

обеспечение координации деятельности субъектов КИИ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

НКЦКИ возглавляет:

директор НКЦКИ - заместитель руководителя Научно-технической службы - начальник Центра защиты информации и специальной связи ФСБ России

Приказ ФСБ России № 366: задачи



Приказ ФСБ России № 366: полномочия

Направляет уведомления и запросы субъектам КИИ и не только

Заключает соглашения о сотрудничестве

Создает рабочие группы из представителей субъектов КИИ для решения вопросов в компетенции НКЦКИ

Привлекает к реагированию на инциденты организации и экспертов

Участвует в различных мероприятиях, связанных с ГосСОПКА

Приказ ФСБ России № 367

Приказ ФСБ России от 24.07.2018 № 367 об утверждении Перечня информации, представляемой в ГосСОПКА, и Порядка представления информации в ГосСОПКА

Перечень информации, предоставляемой в ГосСОПКА

Порядок предоставления информации в ГосСОПКА

Приказ № 367: перечень информации

Информация из реестра ФСТЭК России о ЗОКИИ

Информация о результатах госконтроля

Информация от ФСТЭК России по «не значимым»

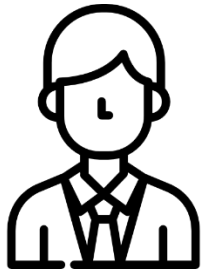
Информация от субъектов КИИ по инцидентам, связанным с функционированием объектов КИИ

Приказ № 367: информация от субъектов КИИ

- дата, время, место нахождения или географическое местоположение объекта КИИ, на котором произошел инцидент
- наличие причинно-следственной связи между инцидентом и атакой
- связь с другими инцидентами (при наличии)
- **состав технических параметров инцидента**
- последствия компьютерного инцидента

Приказ № 367: сроки предоставления информации

по инцидентам, связанным с функционированием объекта КИИ



Субъект КИИ

Направляет информацию об инциденте не позднее 24 часов с момента его обнаружения

уведомляет о получении информации не позднее 24 часов

НКЦКИ

Внимание: в утвержденных приказах ФСБ России нет деления на значимые и не значимые объекты КИИ

Приказ № 367: перечень информации

Иная информация в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты представляется в ГосСОПКА **в сроки**, достаточные для своевременного проведения мероприятий

Попытки - это тоже инциденты

12 типов инцидентов

в методических рекомендациях ФСБ России к центрам ГосСОПКА

21 тип инцидентов

new:

- Попытки внедрения модулей вредоносного ПО
- Попытки эксплуатации уязвимости
- Попытки авторизации в информационном ресурсе

Категории и типы инцидентов: обновленный перечень

КАТЕГОРИЯ ИНЦИДЕНТА	ТИПЫ ИНЦИДЕНТОВ
Внедрение вредоносного ПО	Заражение ВПО
Распространение вредоносного ПО	Использование контролируемого ресурса для распространения или управления модулями ВПО **Попытки** внедрения модулей ВПО
Нарушение или замедление работы контролируемого информационного ресурса	Компьютерная атака типа «отказ в обслуживании» Распределенная компьютерная атака типа «отказ в обслуживании» Контролируемый несанкционированный вывод системы из строя Контролируемое отключение системы (без злого умысла)
НСД в систему	Успешная эксплуатация уязвимости Компрометация учетной записи
Попытки НСД в систему или к информации	**Попытки** эксплуатации уязвимости **Попытки** авторизации в информационном ресурсе
Сбор сведений с использованием информационно-коммуникационных технологий	Сканирование информационного ресурса Прослушивание (захват) сетевого трафика Социальная инженерия
Нарушение безопасности информации	Несанкционированное разглашение информации Несанкционированное изменение информации
Распространение информации с неприемлемым содержимым	Рассылка незапрашиваемых электронных сообщений Публикация запрещенной законодательством РФ информации
Мошенничество с использованием информационно-коммуникационных технологий	Злоупотребление при использовании информационного ресурса Публикация мошеннического информационного ресурса
Наличие уязвимости или недостатков конфигурации в информационном ресурсе	Наличие уязвимости или недостатков конфигурации в информационном ресурсе

Общий знаменатель с CERT-community

INCIDENT CLASSIFICATION	INCIDENT EXAMPLES	DESCRIPTION
Abusive Content	Spam	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content
	Harmful Speech	Discreditation or discrimination of somebody (e.g. cyber stalking, racism and threats against one or more individuals)
	Child/Sexual/Violence/ ...	Child pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	
	Rootkit	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.).
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	New attack signature	An attempt using an unknown exploit.
Intrusions	Privileged account compromise	A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access. Also includes being part of a botnet.
	Unprivileged account compromise	
	Application compromise	
	Bot	
Availability	DoS	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) – or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.
	DDoS	
	Sabotage	
	Outage (no malice)	
Information Content Security	Unauthorised access to information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore, attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/software error can also be the cause.
	Unauthorised modification of information	
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Offering or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
	Phishing	Masquerading as another entity in order to persuade the user to reveal a private credential.
Vulnerable	Open for abuse	Open resolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus signatures not up-to-date, etc
Other	All incidents which do not fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.
Test	Meant for testing	Meant for testing

Table 1: eCSIRT.net mkVI

Приказ № 367: способы взаимодействия

С использованием технической инфраструктуры НКЦКИ

Посредством:

- Почтовой
- Факсимильной
- Электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте http://cert.gov.ru

Важно: Информация об инциденте направляется субъектом КИИ в НКЦКИ не позднее 24 часов с момента обнаружения

Приказ ФСБ России № 368

Приказ ФСБ России от 24.07.2018 № 368 об утверждении
Порядка обмена информацией о компьютерных инцидентах

Порядок обмена информацией
о компьютерных инцидентах между
субъектами КИИ

Порядок получения субъектами КИИ
информации о средствах и способах
проведения компьютерных атак
и о методах их предупреждения
и обнаружения

Приказ ФСБ России № 368: порядок обмена

Субъекты КИИ вправе самостоятельно определять круг субъектов КИИ для обмена

Обмен информацией происходит в сроки, достаточные для своевременного проведения мероприятий

Одновременно в рамках обмена субъекты КИИ информируют НКЦКИ

Приказ ФСБ России № 368: порядок получения информации

Способ №1: по запросу

- cert.gov.ru
- НКЦКИ
  ответ в 5-дневный срок
- ФСБ России
- другие субъекты КИИ

Способ №2: рассылки НКЦКИ

не позднее

24 часов

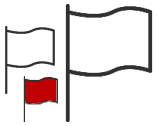
с момента получения информации об атаках НКЦКИ делает рассылку

Источники информации для ГосСОПКА

ГОССОПКА

Субъекты КИИ

Иные органы и организации
(центры ГосСОПКА?)



Иные иностранные организации
(киберцентры других государств?)

POSITIVE TECHNOLOGIES

Построение центров ГосСОПКА

Кто может построить центр ГосСОПКА

Субъекты КИИ

Организации для собственных нужд

Организации, включенные в План развертывания ведомственных сегментов ГосСОПКА, утвержденный Президентом РФ 21.08.2015 г. №9397

Организации-лицензиаты, для оказания услуг

Условия подключения к ГосСОПКА

Субъекты КИИ

по требованиям 187-ФЗ

Организации-лицензиаты,
для оказания услуг

Организации
для собственных нужд

Необходимо стать **субъектом ГосСОПКА**:

- заключить соглашение с ФСБ России,
- выполнить требования для центров ГосСОПКА

Нормативная база для центров ГосСОПКА

- **Требования к подразделениям и должностным лицам** субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ДСП)
- **Методические рекомендации по обнаружению компьютерных атак** на информационные ресурсы Российской Федерации (к)
- **Методические рекомендации по установлению причин и ликвидации последствий** компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации (к)
- **Методические рекомендации по проведению мероприятий** по оценке степени защищенности от компьютерных атак
- **Регламент взаимодействия** подразделений Федеральной службы безопасности Российской Федерации и организации при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак

Субъект ГосСОПКА

СУБЪЕКТЫ ГОССОПКА —

государственные органы РФ, 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

Субъекты ГосСОПКА — не только субъекты КИИ

Условия для создания центра ГосСОПКА

Получить лицензии:

- ФСБ России на право осуществления работ, связанных с использованием сведений, составляющих гос.тайну (в случае если обрабатывается ГТ)
- ФСТЭК России на деятельность по ТЗКИ (по части мониторинга)
- Одну из лицензий ФСБ России на право:
  - осуществления работ, связанных с созданием СЗИ, содержащей сведения, составляющие гостайну;
  - деятельности, связанной с шифровальными средствами.

Разработать документы:

- Положение о центре ГосСОПКА
- Регламент деятельности центра
- Штатное расписание центра

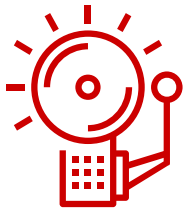
Заключить соглашение

с ФСБ России о взаимодействии с ГосСОПКА

POSITIVE TECHNOLOGIES

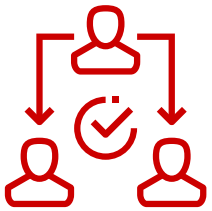
Порядок выполнения требований по ГосСОПКА для субъектов КИИ

Даже если нет значимых объектов КИИ…



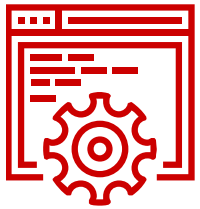
Незамедлительно информировать

ФСБ России
об инцидентах



Оказывать содействие

должностным лицам
ФСБ России



Обеспечивать выполнение

порядка, технических условий установки и эксплуатации средств ГосСОПКА, если они устанавливаются на его объектах КИИ

Выбираем путь

Есть значимые объекты КИИ

Непрерывное взаимодействие
с ГосСОПКА

Нет значимых объектов КИИ

Информирование ФСБ России
об инцидентах

Порядок взаимодействия один и тот же

Что делать субъектам КИИ

1. Разработать регламент информирования с указанием конкретных сроков информирования ФСБ России об инцидентах

2. В случае подключения к технической инфраструктуре НКЦКИ направить запрос в НКЦКИ (gov-cert@gov-cert.ru) о необходимости организации технической возможности по незамедлительному информированию о компьютерных инцидентах в соответствии с частью 2 статьи 9 ФЗ-187

3. Подключиться к технической инфраструктуре НКЦКИ в соответствии с установленном порядком

4. Информировать об инцидентах

POSITIVE TECHNOLOGIES

Спасибо за внимание