КСБ-СОФТ

Ответы на насущные вопросы по информационной безопасности объектов КИИ. Часть 5

Спикеры:

- **Максим Шляпкин –** руководитель отдела защиты объектов КИИ и АСУ ТП
- **Александр Кирий –** руководитель центра мониторинга SOCRAT

Модератор:

- **Дмитрий Чирков –** руководитель регионального направления

КСБ-СОФТ

- Лицензиат ФСТЭК России
- Лицензиат ФСБ России

Входим в ГК «Кейсистемс»

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

80+
регионов внедрения

6000+
реализованных проектов

Портфолио КСБ-СОФТ

Обменивайтесь
сообщениями
во вкладке «Чат»

Запись вебинара
направим всем
участникам на указанный
при регистрации e-mail

Задавайте вопросы
во вкладке «Вопросы»

Темы для обсуждения

- выполнение новых требований
по взаимодействию с ГосСОПКА
- применение перечней отраслевых
объектов КИИ и отраслевых особенностей
категорирования
- оценка показателя состояния технической
защиты информации и обеспечения
безопасности значимых объектов КИИ

Ответы на вопросы

Вопрос № 1

В отраслевых особенностях категорирования прописаны формулы расчета показателя 8 и 9, но ранее в организации была выпущена своя методика расчета этих показателей, по которой все это время и работали. Вопрос: обязательно ли сейчас переходить на формулы, представленные в отраслевых особенностях или можно продолжать использовать свои?

Отраслевые особенности категорирования

Часть 4 статьи 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

"Субъекты КИИ в соответствии с критериями значимости и показателями их значений, порядком осуществления категорирования, перечнями типовых отраслевых объектов КИИ и **отраслевыми особенностями категорирования объектов КИИ** присваивают одну из категорий значимости принадлежащим им на праве собственности, аренды или ином законном основании объектам КИИ. Если объект КИИ не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий."

Пункт 6[1] ПП РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

Установление соответствия объекта КИИ критериям значимости и показателям их значений, расчет значений показателей критериев значимости с учетом особенностей функционирования объекта КИИ и присвоение ему одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения такой категории осуществляются в соответствии с настоящими Правилами и **отраслевыми особенностями категорирования объектов КИИ, предусмотренными пунктом 5 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" (далее - отраслевые особенности категорирования).**

Вопрос № 2

Интересуют новшества в требованиях к взаимодействию с ГосСОПКА

Взаимодействие с ГосСОПКА

В декабре 2025
опубликовано 7 приказов ФСБ России

Регламентирующие взаимодействие:

№539 Порядок получения субъектами КИИ информации о средства и способах КА и методах предупреждения

№546 Порядок обмена информации о КА и КИ между субъектами КИИ

№547 Порядок информирования о КА и КИ

№548 Порядок осуществления непрерывного взаимодействия субъектов КИИ с ГосСОПКА

Приказ ФСБ России от 23.12.2025 № 539

«Об утверждении Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

Субъекты КИИ обязаны получать информацию о средствах и способах проведения КА и о методах их предупреждения:

- На сайте НКЦКИ (https://cert.gov.ru/);
- Направления запросов в НКЦКИ с использованием ТИ НКЦКИ, либо посредством почтовой или электронной связи (ответ предоставляется в течение 30 р.д.);
- Получения от НКЦКИ информации о средствах и способах проведения КА и о методах их предупреждения и обнаружения.

Материалы

Правовые основания

Уведомления об уязвимостях программного обеспечения (УПО)

Уведомления об угрозах безопасности информации

Документы о взаимодействии

https://safe-surf.ru/specialists/alrt-nkcki/ - Бюллетени НКЦКИ: уведомление об угрозах
https://safe-surf.ru/specialists/bulletins-nkcki/ - Бюллетени НКЦКИ: уведомление об уязвимости ПО

Приказы ФСБ России от 25.12.2025 № 546, 547, 548

«Об утверждении Порядка обмена информацией о КА и КИ 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 КИ»

Уведомлять НКЦКИ нужно как о КИ, так и о КА:

Субъекты КИИ о КИ

3 часа – для ЗОКИИ
24 часа – для иных ОКИИ

Субъекты КИИ о КА

24 часа

Субъекты КИИ, имеющие ЗО КИИ, обязаны осуществлять непрерывное взаимодействие с НКЦКИ и передавать информацию о КА и КИ через ТИ НКЦКИ:

С использованием линейки продуктов ViPNet компании Инфотекс (номер сети ViPNet: 10976)

С использованием линейки продуктов аппаратно-программного комплекса шифрования «Континент» производства ООО «Код Безопасности»

С использованием линейки продуктов S-Terra производства ООО «С-Терра СиЭсПи»

С использованием линейки продуктов ЗАСТАВА производства АО «ЭЛВИС-ПЛЮС»

Вопрос № 3

Что делать в такой ситуации: в начале 2025 года создан новый объект, категория значимости не присвоена. После выхода нового показателя 13.1 при пересмотре категории этот объект становится значимым, но требования по ДПАК не выполнены. В соответствии с ПП 1912 нельзя использовать ПАК, не являющиеся доверенными, купленные после 01.09.2024 на ЗОКИИ. Получается пока не будет все импортозамещено объект нужно законсервировать? Как быть в такой ситуации?

Рекомендации:

1. Провести оценку угроз для данного объекта КИИ, сформировать требования к системе обсепечения информационной безопасности (СОИБ)
2. Осуществить проектирование СОИБ объекта КИИ
3. Внедерить и испытать СОИБ объекта КИИ
4. Разработать план перехода на доверенные ПАК
5. Если для объекта КИИ невозможно подобрать доверенные ПАК из-за отсутствия российских аналогов, необходимо получить заключение Минпромторга РФ об отнесении продукции к промышленной продукции, не имеющей произведённых в РФ аналогов. Это позволит временно продолжать использование существующих решений

Импортозамещение

Постановление Правительства РФ от 20 сентября 2017 г. N 1135

"Об отнесении продукции к промышленной продукции, не имеющей произведенных в Российской Федерации аналогов, и внесении изменений в некоторые акты Правительства Российской Федерации"

- **критерии отнесения продукции к промышленной продукции, не имеющей произведенных в Российской Федерации аналогов;**
- **правила отнесения продукции к промышленной продукции, не имеющей произведенных в Российской Федерации аналогов;**
- требования к организациям, осуществляющим экспертизу определения отличий параметров продукции от параметров российской промышленной продукции;
- правила проведения отбора организаций, осуществляющих экспертизу определения отличий параметров продукции от параметров российской промышленной продукции;
- методика определения размера платы за оказание необходимой и обязательной услуги по экспертизе определения отличий параметров продукции от параметров российской промышленной продукции;
- предельный размер платы за оказание необходимой и обязательной услуги по экспертизе определения отличий параметров продукции от параметров российской промышленной продукции

Вопрос № 4

Какие именно события ИБ и с какой периодичностью нужно направлять в ГосСОПКА по новым требованиям?

Как отличить инцидент, подлежащий обязательной передаче, от обычного алерта SIEM, и какие поля в отчёте являются критическими (чтобы не получить возврат от НКЦКИ)?

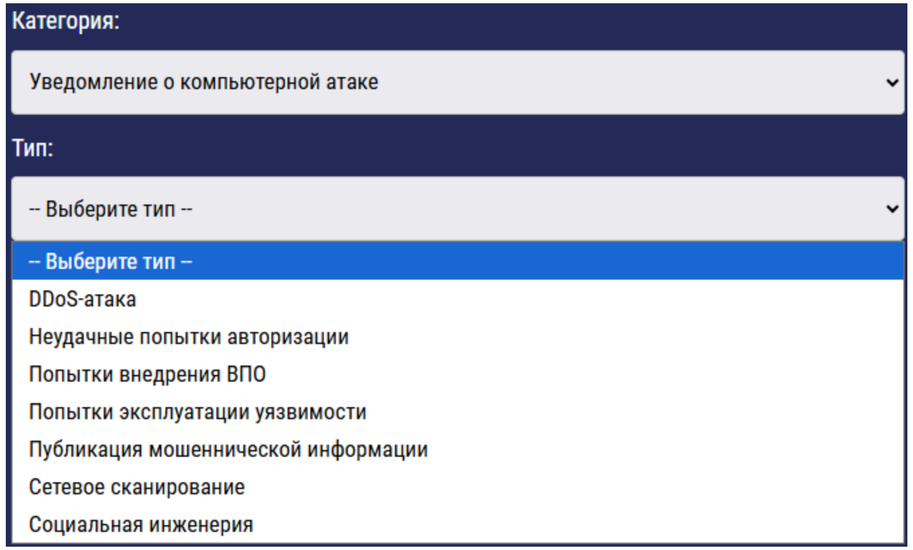
Какие именно события ИБ и с какой периодичностью нужно направлять в ГосСОПКА по новым требованиям?

Уведомлять НКЦКИ нужно о компьютерных атаках (**КА**) и компьютерных инцидентах (**КИ**)

КИ – события связанные с нарушением штатного режима работы, в том числе, не связанные с компьютерными атаками.

КА – компьютерные атаки направленные на контролируемые объекты

Для каждого КИ и КА есть свои типы:



Для ЗОКИИ
отправка уведомлений
в течение 3 часов

на КИ и 24 часа на КА;

Для остальных
объектов,
- 24 часа на КИ и КА.

Какую категорию выбрать?

Категория "Уведомление о компьютерном инциденте" выбирается в случае, если нарушен штатный режим работы объекта в зоне ответственности организации, указанной в поле «Владелец информационного ресурса» (далее – Объект) и/или безопасность обрабатываемой таким Объектом информации. В соответствии с законодательством, такое событие должно быть классифицировано как "компьютерный инцидент", даже если событие не связано с компьютерной атакой. Нештатное функционирование может быть вызвано, в том числе, проблемами со связью, возникшими в зоне ответственности оператора связи.

Категория "Уведомление о компьютерной атаке" выбирается в случае выявления компьютерных атак, направленных на Объекты, не приведших к нарушению их штатного функционирования или безопасности обрабатываемой информации.

https://cert.gov.ru/uvedomlenie.php

Как отличить инцидент, подлежащий обязательной передаче, от обычного алерта SIEM?

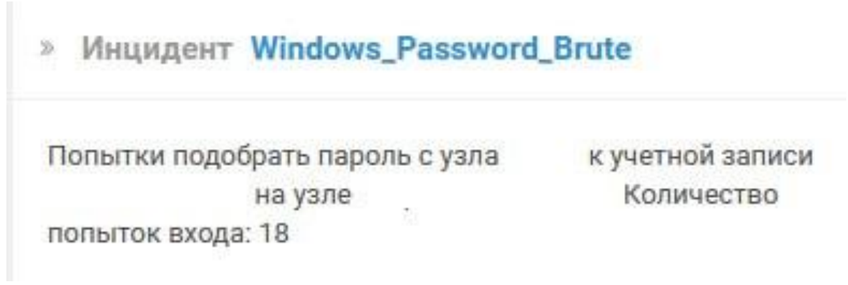
Если события ИБ можно попадает под КА и/или КИ в соответствии с классификацией НКЦКИ, то нужно отправлять в ГосСОПКА

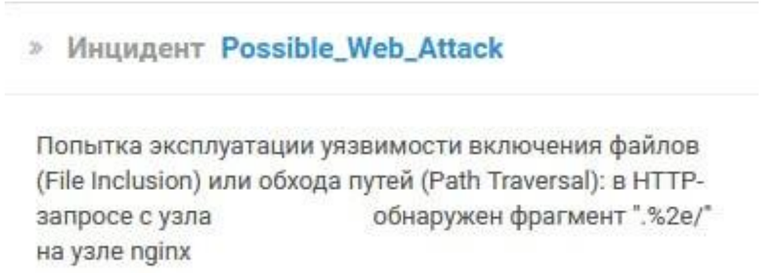
Типы КА

DDoS-атака
Неудачные попытки авторизации
Попытки внедрения ВПО
Попытки эксплуатации уязвимости
Публикация мошеннической информации
Сетевое сканирование
Социальная инженерия

Типы КИ

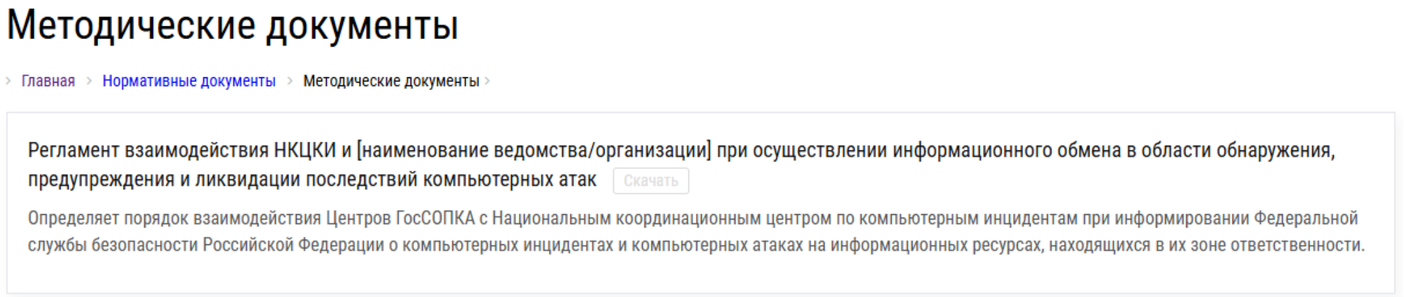
Использование контролируемого ресурса для проведения атак
Замедление работы ресурса в результате DDoS-атаки
Заражение ВПО
Захват сетевого трафика
Компрометация учетной записи
Несанкционированное изменение информации
Несанкционированное разглашение информации
Публикация на ресурсе запрещенной законодательством РФ информации
Успешная эксплуатация уязвимости
Событие не связано с компьютерной атакой





Какие поля в отчёте являются критическими (чтобы не получить возврат от НКЦКИ)?

Под каждый тип КА и/или КИ есть отдельные уникальные поля



https://gossopka.ru/upload/iblock/9be/l71g1vhv5zvquvtwo9rzp3bljn6xmjhu/Reglament-informatsionnogo-vzaimodeystviya.pdf

На сайте НКЦКИ есть конструктор по формированию обращения для отправки на почту (https://cert.gov.ru/uvedomlenie.php)

В личном кабинете ГосСОПКА, при создании обращения указан набор обязательных полей

Состав полей карточки указан в приложении к регламенту

Таблица 1 – Сведения о субъекте КИИ
Общая информация о субъекте КИИ

Таблица 2 – Сведения о КА и КИ
Информация по КА и/или КИ

Общие сведения	
Категория	Уведомление о компьютерной атаке
Тип события ИБ	DDoS-атака

Общие сведения	
Категория	Уведомление о компьютерном инциденте
Тип события ИБ	Использование контролируемого ресурса для проведения атак

Передача мониторинга и взаимодействия с НКЦКИ на аутсорс

Указ Президента РФ №250 от 01 мая 2022 года

Пункт 1 , подпункт в) *принимать в случае необходимости решения о* ***привлечении организаций к осуществлению мероприятий по обеспечению информационной безопасности органа (организации)***.
При этом могут привлекаться исключительно организации, имеющие лицензии на осуществление деятельности по технической защите конфиденциальной информации.

SOCRAT – центр мониторинга и реагирования на инциденты информационной безопасности компании КСБ-СОФТ

- Функционирует 24x7
- Работает в соответствии с требованиями регулятора (117, 239 приказы ФСТЭК России, ГОСТ Р 59547-2021, иные)
- Использует данные об актуальных угрозах для раннего обнаружения неизвестных атак
- Имеет гибкий подход предоставления услуг (исходя из потребностей)
- Как сервисное, так и гибридное оказание услуг
- Является корпоративным центром ГосСОПКА (класс А)

Работаем с региональными органами исполнительной власти и их подведомственные учреждения с 2022 года:

- Министерства финансов
- Министерства здравоохранения и аналитические центры (МИАЦ, больницы)
- Министерства труда
- Министерства цифрового развития и аналитические центры
- Коммерческие организации

Вопрос № 5

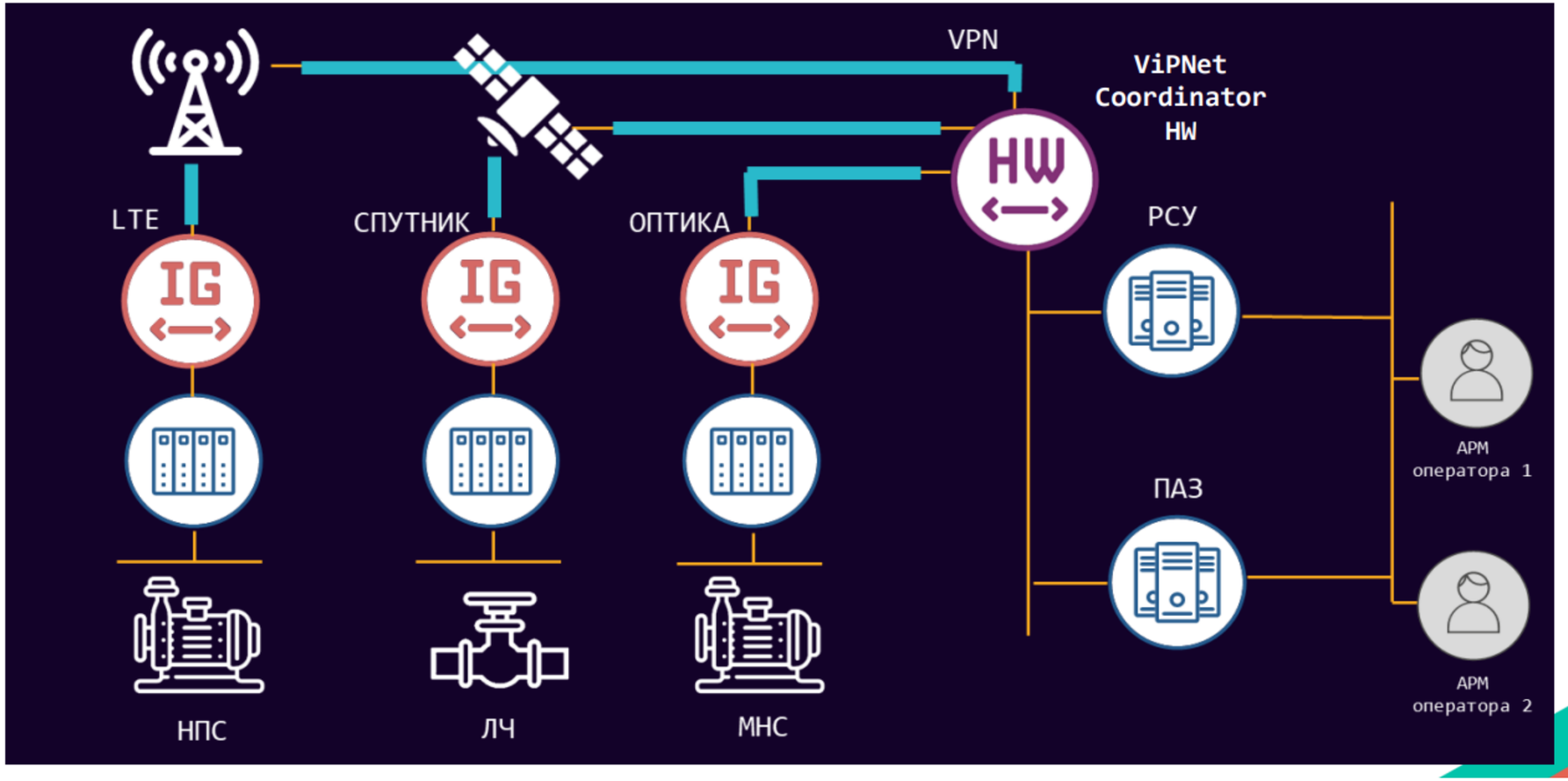
ЗОКИИ. Тип объекта – АСУ ТП. Архитектура объекта - клиент-серверная. Общая сеть линий связи сервера с периферийными устройствами территориально распределена в радиусе более 200 км. Прием/передача данных осуществляется по собственным линиям связи (оптоволокно), через интернет (провайдер) и 3G. Телекоммуникационного и периферийного оборудования более 6 000 ед. Протяженность линий связи (оптоволокна) более 1000 км.

Вопрос 1. Как обеспечить защиту линейного, географически распределенного объекта, его линий связи (оптоволокна), коммутационных и периферийных устройств?

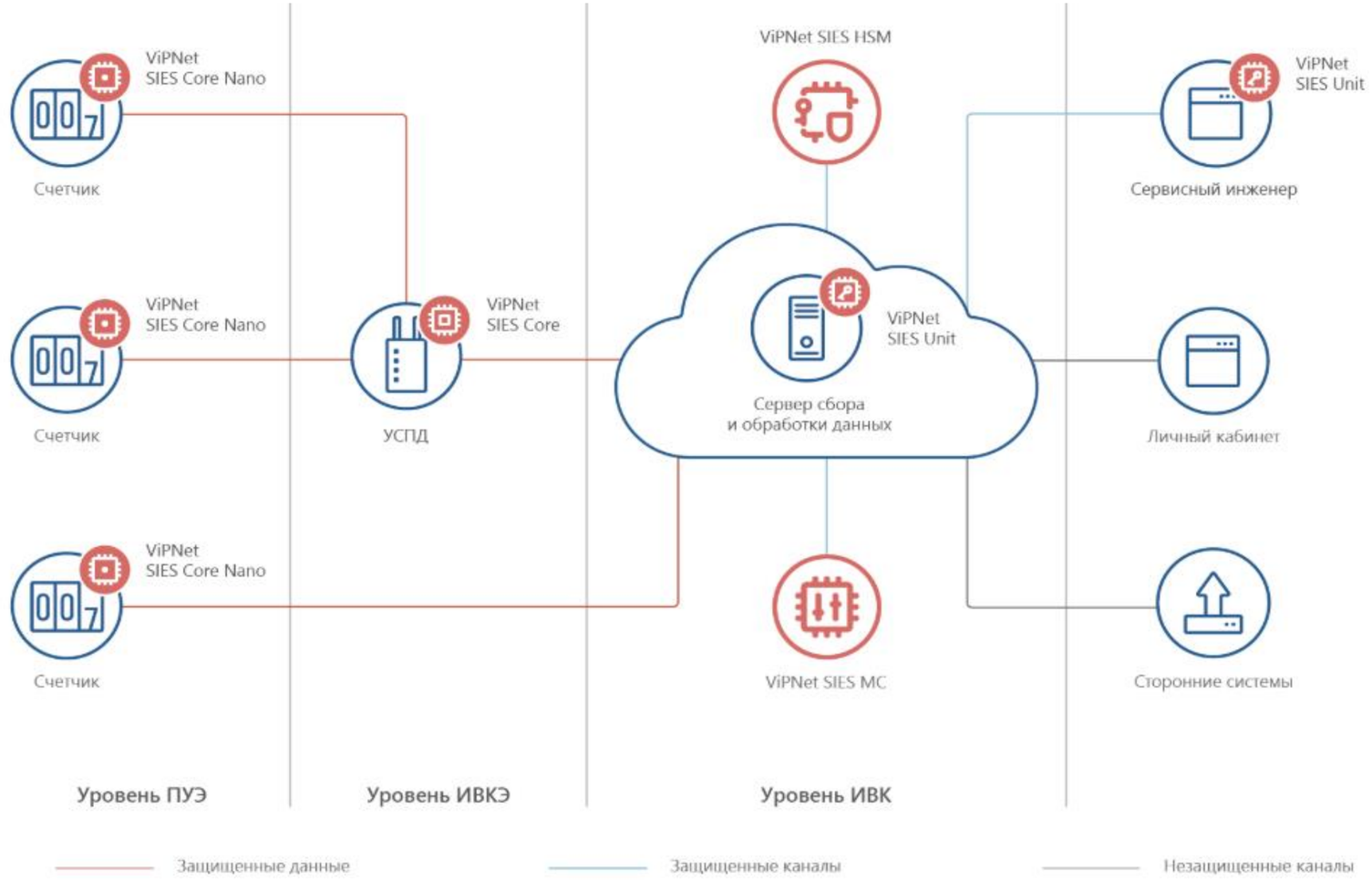
Вопрос 2. Можно ли ограничиться защитой оборудования размещенного в контролируемой зоне (серверная, АРМ)?

Защита каналов связи с помощью продуктов «ИнфоТеКС»

VPN для распределенных объектов



Защита каналов связи с помощью продуктов «ИнфоТеКС»



Защищенная ИСУЭ

Вопрос № 6

После вступления в силу Распоряжения Правительства РФ от 26 февраля 2026 г. № 360-р прошу разъяснить: является ли станок с ЧПУ объектом КИИ, или, согласно Типового перечня объектами являются ИС, ИТКС и АСУ ТП которые обеспечивают управление станком (например п.158, 159 Распоряжения). Станок с ЧПУ, отдельно стоящий (без сетей, без АСУ, без ИС), является объектом КИИ?

Промышленное оборудование (станки с ЧПУ, климатические камеры) попадающее под пункт 222, 238 Перечня типовых ОКИИ, являются ли ОКИИ как самостоятельное оборудование или же ОКИИ будет АСУ управляющее неким парком данных станков?

Перечень типовых отраслевых объектов КИИ

158.	Информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, обеспечивающие управление оборудованием (станками) с числовым программным управлением	управление процессом производства изделий;
		Автоматизация управления технологическим оборудованием (агрегатами, установками (группами станков) и отдельными станками), реализующим самостоятельный технологический процесс;
		Управление оборудованием, в том числе роботизированным оборудованием, для получения полуфабрикатов, деталей, сборочных единиц и прочего;
		Передача информации о проектируемой продукции в целях ее дальнейшего производства;
		Управление подготовкой управляющих программ для станков с числовым программным управлением
159.	Автоматизированные системы управления, предназначенные для управления парком оборудования (парком станков)	Управление процессом производства изделий;
		Управление процессом качества изделий

222.	Информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, предназначенные для управления станками с числовым программным управлением	Управление обрабатывающими станками с программным обеспечением, которое позволяет задавать станку определенный набор параметров для обработки деталей в автоматическом режиме (фрезерные, токарные, токарно-карусельные, шлифовальные, зуборезьбообрабатывающие, горизонтально-расточные)
238.	Информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, предназначенные для управления испытательными стендами	Обеспечение различных приемочных, контрольных специальных испытаний различных объектов, при поведении которых объект подвергается воздействию нагрузок, сопоставимых или превышающих таковые в реальных условиях;

Автоматизированная система управления — это комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами (187-ФЗ)

Вопрос № 7

Как выстроить процесс эскалации внутри организации, чтобы соблюсти сроки передачи сведений в ГосСОПКА, если часть артефактов собирается вручную?

Как выстроить процесс эскалации внутри организации, чтобы соблюсти сроки передачи сведений в ГосСОПКА, если часть артефактов собирается вручную?

Процесс реагирования на КА и КИ должен быть описан в Плане реагирования на КА и КИ

https://gossopka.ru/upload/iblock/a9f/3va55amvsxqelhuo1oufo9y6998nbtwz/Metodicheskie-rekomendatsii-po-razrabotke-Plana-reagirovaniya.pdf - *Методические рекомендации по разработке Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации*

3, либо 24 часа – срок уведомления НКЦКИ о подозрении на КА и/или КИ с момента обнаружения

48 часов – срок уведомления НКЦКИ о результатах по реагированию и принятию мер по ликвидации

Сроки реагирования и принятия мер – регламентируются во внутреннем Плане реагирования на КА и КИ

В плане реагирования могут быть указаны сроки позволяющие проводить работы по сбору информации (в т.ч. артефактов).

Как выстроить процесс эскалации внутри организации, чтобы соблюсти сроки передачи сведений в ГосСОПКА, если часть артефактов собирается вручную?

Распределить роли

Ответственное лицо за выявление КИ и реагирование на них – отвечает за реализацию и функционирования процесса. Координирует действия, взаимодействует с командами и регулятором;

Аналитик/администратор безопасности – специалисты отвечающие за мониторинг событий поступающих в SIEM-систему, корректировку правил для снижения кол-ва ложных сработок, добавление контента (бюллетени НКЦКИ, индикаторы из писем ФСТЭК и прочее), создание карточек инцидентов и отправку рекомендаций службе ИТ для устранения выявленных угроз безопасности

Дополнительно: контроль работоспособности системы мониторинга и источников событий. В случае нарушения – отвечают за отправку заявки в службу ИТ;

Служба ИТ/ответственный за эксплуатацию ЗОКИИ – специалисты отвечающие за работоспособность систем мониторинга и источников событий, выполнение рекомендаций аналитиков связанных с угрозами безопасности.

№	Мероприятие	Время реализации	Ответственное лицо
1	Регистрация		
2	Информирование НКЦКИ	3 часа с момента регистрации	
3	Анализ КИ, установление связи с КА и определение действий по реагированию		
4	Определение состава лиц ответственных за реагирование на КИ и принятие мер по ликвидации последствий		
5	Определение перечня средств для принятия мер по ликвидации		
6	Определение очередности ОКИИ, в отношении которых будут приниматься меры по ликвидации		
7	Определение перечня мер по восстановлению функционирования		
8	Устранение причин, условий и последствий по восстановлению функционирования		
9	Информирование НКЦКИ о результатах	48 часов после выполнения п.8	
10	Разработка предложений по улучшению СИБ		

Вопрос № 8

Какие существуют особенности категорирования субъектов КИИ металлургической промышленности?

Отраслевые особенности категорирования в сфере металлургической промышленности (проект)

- три условия отнесения субъекта КИИ к сфере металлургической промышленности;
- отраслевые признаки значимости;
- перечень показателей критериев значимости, которым необходимо уделить особое внимание;
- правила определения показателя «причинение ущерба жизни и здоровью людей (человек)»;
- правила и формулы для определения показателя «возникновение ущерба субъекту КИИ, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, организацией оборонно-промышленного комплекса, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процент от годового объема доходов, усредненного за прошедший 5-летний период)»
- правила и формулы для определения показателя «возникновение ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет, осуществляемых субъектом КИИ (процент прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период)»

Вопрос № 9

Вопрос по Методике оценки показателя состояния технической защиты информации в ИС и обеспечения безопасности ЗОКИИ РФ.

Верно ли мы понимаем, что если в организации функционирует несколько ОКИИ, то необходимо отдельно для каждого из них определять значения частных показателей, далее на основании значений данных показателей определять общий показатель защищенности Кзи на всю организацию?

Ответ ФСТЭК России

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК России)

Старая Басманная, д. 17, Москва, 105066
Тел., факс: (495) 696-49-04
E-mail: postin@fstec.ru

8 12 2025 № 240/92/6838

На №

М.С.ШЛЯПКИНУ
[redacted]

О рассмотрении обращения

Уважаемый Максим Сергеевич!

Обращение по вопросу оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (далее — Показатель защищенности) в ФСТЭК России рассмотрено.

Пунктом 31 Методики оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденной ФСТЭК России 11 ноября 2025 г., определено, что частные показатели безопасности k_{ji} определяются для всех информационных систем, подлежащих защите в соответствии с нормативными правовыми актами Российской Федерации, находящихся в распоряжении органа (организации).

При этом в случае если по результатам расчета для указанных информационных систем получены различные значения по одной и той же группе частных показателей безопасности, то при расчете Показателя защищенности необходимо учитывать минимальное значение частных показателей безопасности.

Показатель защищенности определяется для информационной инфраструктуры органа (организации), в которой функционируют информационные (автоматизированные) системы.

Проект приказа ФСТЭК России от 07.04.2025 о внесении изменений в приказы ФСТЭК России № 235 и 239

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

___ апреля 2026 г. Москва № ____

О внесении изменений в приказы Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 и от 25 декабря 2017 г. № 239

В соответствии с пунктами 3 и 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», абзацем первым пункта 2, а также подпунктами 6^1 и 6^2 пункта 8 Положения о Федеральной службе по экспортному и техническому контролю, утвержденного Указом Президента Российской Федерации № 1085, **П Р И К А З Ы В А Ю**:

1. Утвердить прилагаемые изменения, которые вносятся в приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 (зарегистрирован Минюстом России 22 февраля 2018 г., регистрационный № 50118), с изменениями, внесенными приказами ФСТЭК России от 27 марта 2019 г. № 64 (зарегистрирован Минюстом России 13 июня 2019 г., регистрационный № 54920) и от 20 апреля 2023 г. № 69 (зарегистрирован Минюстом России 23 июня 2023 г., регистрационный № 73969),
и в приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 (зарегистрирован Минюстом России 26 марта 2018 г., регистрационный № 50524), с изменениями, внесенными приказами ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071), от 26 марта 2019 г. № 60 (зарегистрирован Минюстом России 18 апреля 2019 г., регистрационный № 54443), от 20 февраля 2020 г. № 35 (зарегистрирован Минюстом России 11 сентября 2020 г., регистрационный № 59793), от 28 августа 2024 г. № 159 (зарегистрирован Минюстом России 24 октября 2020 г., регистрационный № 79900).

2. Настоящий приказ вступает в силу с 1 сентября 2026 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Утверждены
приказом ФСТЭК России
от «___» апреля 2026 г. № ____

Изменения,
которые вносятся в приказы Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 и от 25 декабря 2017 г. № 239

1. Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом ФСТЭК России
от 21 декабря 2017 г. № 235, дополнить пунктом 36^1 следующего содержания:

«36^1. В рамках контроля состояния безопасности значимых объектов критической информационной инфраструктуры должен проводиться расчет:

а) показателя, характеризующего текущее состояние обеспечения безопасности значимых объектов критической информационной инфраструктуры
от базового уровня угроз безопасности информации (далее — показатель защищенности $К_{зи}$);

б) показателя, определяющего достаточность и эффективность проведенных мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры (далее — показатель уровня зрелости $П_{зи}$).

Для определения значений и расчета показателя защищенности $К_{зи}$ и показателя уровня зрелости $П_{зи}$ должны применяться методические документы, утвержденные ФСТЭК России в соответствии с абзацем вторым пункта 5 и подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (далее — методические документы ФСТЭК России).

Расчет и оценка показателя защищенности $К_{зи}$ проводится не реже одного раза в шесть месяцев. Расчет и оценка показателя уровня зрелости $П_{зи}$ проводится не реже одного раза в два года.

О полученных по результатам оценки значениях показателя защищенности $К_{зи}$ и показателя уровня зрелости $П_{зи}$ в случае их несоответствия нормированным значениям, указанным в методических документах ФСТЭК России, в течение
3 календарных дней со дня завершения такой оценки информируется руководитель субъекта критической информационной инфраструктуры для принятия решения о проведении дополнительных мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

Оценка показателя состояния технической защиты информации и обеспечения безопасности ЗОКИИ

Работы

Экспертный аудит для сбора исходных данных, необходимых для оценки показателя защищенности

Анализ уязвимостей устройств и интерфейсов, доступных из сети Интернет, а также пользовательских устройств и серверов

Регламентация оценки показателя технической защищенности

Проведение оценки показателя защищенности

Планирование работ по защите информации

Отчётные документы

Отчет о проведении аудита с результатами проведения опроса (интервьюирования) работников и отчетными документами, материалами для отправки регулятору

Отчет об анализе уязвимостей

Регламент оценки показателя технической защищенности

Акт оценки показателя защищенности

План реализации мероприятий по повышению уровня защищенности

КОМПАНИЯ КСБ-СОФТ

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

Обеспечение безопасности КИИ и АСУ ТП

Анализ уязвимостей и тестирование на проникновение

Мониторинг и реагирование на инциденты ИБ

Аудит информационной безопасности

Консалтинг по безопасной разработке и сертификации СЗИ

Оценка показателя состояния технической защиты информации и обеспечения безопасности ЗОКИИ

Наши клиенты – государственные и коммерческие организации в 80 регионах России

На сегодня в портфолио компании более 6000 проектов разной степени сложности, полученный опыт в которых, помогает нам подбирать эффективные решения для защиты информационных ресурсов наших клиентов

РАБОТАЙТЕ С НАМИ!

https://ksb-soft.ru/

428000, г. Чебоксары,
пр-т Максима Горького,
18 Б, пом. 9

8 800 3333-872

info@ksb-soft.ru

Сайт компании

Группа Вконтакте

Телеграм-канал
«Мнение Интегратора»

Канал в MAX
«Мнение Интегратора»