КСБ-СОФТ

С•Терра®

Ответы на насущные вопросы по информационной безопасности объектов КИИ. Часть 4

Спикеры:

- **Максим Шляпкин –** руководитель отдела защиты объектов КИИ и АСУ ТП, КСБ-СОФТ
- **Светлана Семенова –** руководитель группы продвижения продуктов, С-Терра

Модератор:

- **Александр Ильин –** руководитель регионального направления, КСБ-СОФТ

«КСБ-СОФТ»

- Лицензиат ФСТЭК России
- Лицензиат ФСБ России

Телеграм-канал
«Мнение интегратора»

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

80+
регионов внедрения

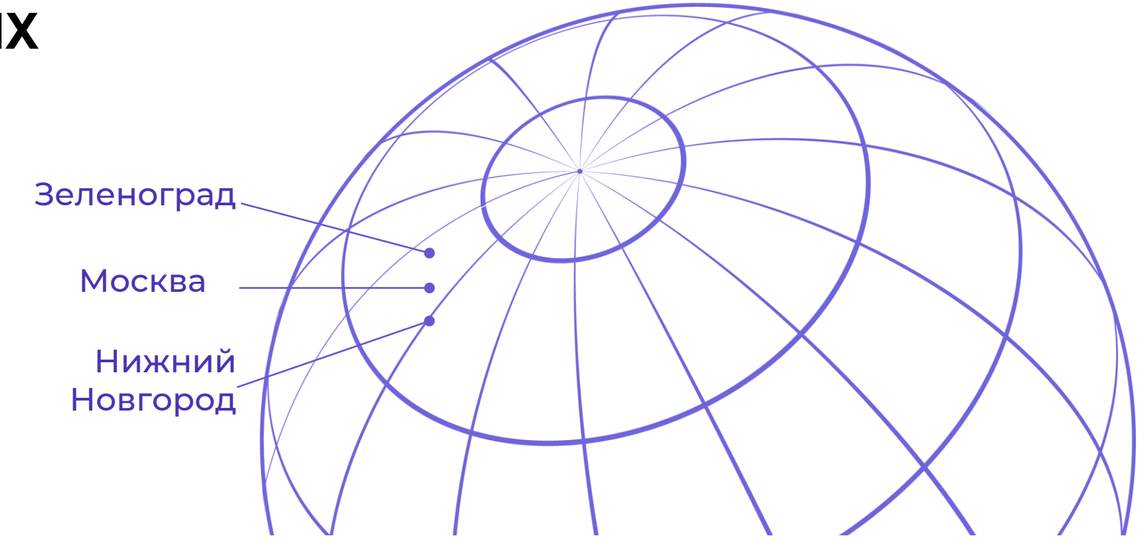
4000+
реализованных проектов

Портфолио КСБ-СОФТ

С-ТЕРРА СИЭСПИ — ЭТО

Разработка и производство **СЕРТИФИЦИРОВАННЫХ** средств защиты каналов связи (VPN, FW, IDS и др.)

КРИПТОГРАФИЧЕСКАЯ защита информации. Лицензиаты **ФСБ** России и **ФСТЭК** России



2003	2006	2008	2010	2012	2014	2017	2020	2024
Основание компании	Разработки с Cisco NME-RVPN	Версия 3.0	Версия 3.1	Версия 3.11	Версия 4.1	Версия 4.2	Версия 4.3	Версия 5.0

Обменивайтесь
сообщениями
во вкладке «Чат»

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

Задавайте вопросы
во вкладке «Вопросы»

Телеграм-канал
«Мнение интегратора»

Темы для обсуждения

- сетевая безопасность и защита каналов связи на объектах КИИ
- проектирование СОИБ объектов КИИ: ключевые этапы и рекомендации
- определение необходимого класса СКЗИ для защиты объектов КИИ
- грядущие изменения в законодательстве – к чему готовиться?
- и многое другое

Наградим авторов 3 лучших вопросов фирменным мерчем!

Цикл вебинаров, посвященных вопросам ИБ в КИИ

Если Вы хотите, чтобы мы подробно разобрали Ваш вопрос на следующем вебинаре, задавайте вопрос по ссылке:

Ответы на вопросы

Вопрос № 1

Прокомментируйте, пожалуйста, последние изменения в 187-ФЗ. Как они повлияют на субъектов КИИ? К чему готовиться?

Федеральный закон от 07.04.2025 № 58-ФЗ «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации».

Изменения вступают в силу 1 сентября 2025 года

ОТРАСЛЕВЫЕ ОСОБЕННОСТИ ОБЪЕКТОВ КИИ

ПРАВИТЕЛЬСТВО РФ УСТАНОВИТ:

- перечни типовых отраслевых объектов КИИ;
- отраслевые особенности категорирования объектов КИИ, определяющие порядок установления критериев значимости и показателей их значений для объектов КИИ, а также порядок расчета значений с учетом особенностей объектов КИИ

Ссылка

ИМПОРТОЗАМЕЩЕНИЕ

ПРАВИТЕЛЬСТВО РФ УСТАНОВИТ:

- требования к программно-аппаратным средствам, используемым на значимых объектах КИИ;
- порядок и сроки перехода на использование требуемых программно-аппаратных средств и отечественного программного обеспечения (ПО);
- порядок осуществления мониторинга за использованием требуемых программно-аппаратных средств и отечественного ПО

ВЗАИМОДЕЙСТВИЕ С НКЦКИ. ГОССОПКА

- необходимо уведомлять ГосСОПКА не только о компьютерных инцидентах, но и о компьютерных атаках;
- ожидаем внесение изменений в приказы ФСБ России № 196, 281, 282, 368;
- ГосСОПКА теперь включает силы иных органов и организаций, не являющихся субъектами КИИ (например, гос. Органов и операторов ПД)

РЕКОМЕНДАЦИИ В СВЯЗИ С НОВОВВЕДЕНИЯМИ

1. Запланировать потенциальные работы по пересмотру объектов КИИ и их категорий значимости — после выпуска соответствующих документов от Правительства Российской Федерации и ФСТЭК России

2. Организовать взаимодействие с ГосСОПКА — самостоятельно или через специализированные центры, имеющие соглашение с НКЦКИ (SOCRAT)

3. Оценить объем используемого импортного ПО и программно-аппаратных средств в составе значимых объектов КИИ

4. Рассчитать примерные бюджеты в части перехода на отечественные решения, запланировать импортозамещение — после утверждения соответствующих документов со стороны Правительства Российской Федерации

Вопрос № 2

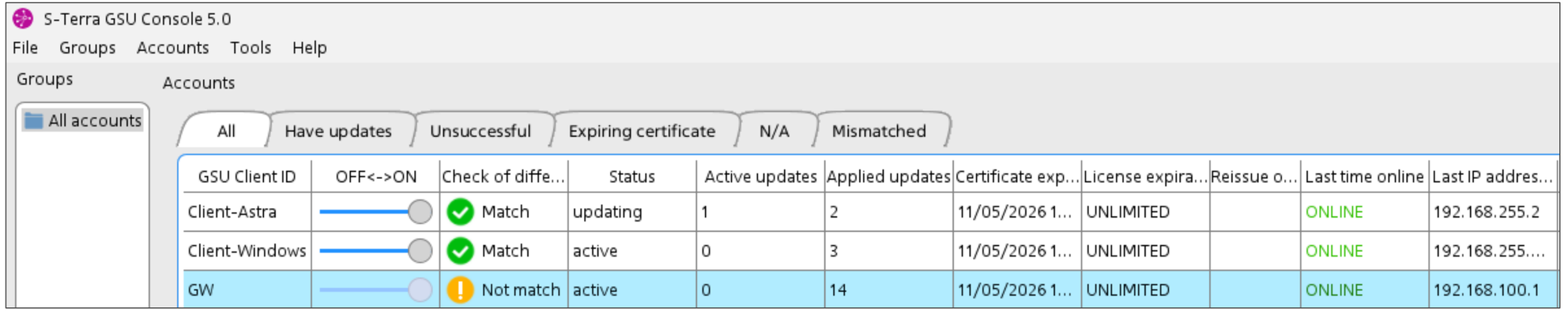
Ранее использовали Microsoft (Службы сертификатов Active Directory) в сочетании с "КриптоПро CSP" для управления сертификатами. Однако в связи со скорым переходом на ОС Astra Linux SE, нам необходимо заменить текущий УЦ.

В связи с этим вопрос: планируется ли выход собственного удостоверяющего центра (УЦ) от С-Терра, который будет совместим с Astra Linux SE? Или есть уже готовые решения для такого случая?

С-ТЕРРА ГСУ (бывш. КП) – МОНИТОРИНГ И УПРАВЛЕНИЕ

Система централизованного управления и мониторинга VPN-устройствами С-Терра

Обновление версий, начиная с версии 4.3



Выпуск сертификатов	Настр. конфигураций	Операционные системы	Мониторинг	Система бэкапов / Опциональность
Интеграция с УЦ Microsoft CA	Механизм защиты от неудачных обновлений	MS Windows Server 2012/2016/2019/2022	CPU, Memory, Network на устройствах	Аналогично снэпшотам в гипервизоре
Собственный УЦ	Групповые операции обновления VPN устройств	Astra Linux 1.7	Оповещение по триггерам	VPN-устройства могут работать без системы управления
Свой УЦ + Автоматическое обновление в 5.0				

[С-Терра ГСУ 5.0]

- ОС Astra Linux, платформа из реестра РЭП
- Автоматическое обновление сертификатов
- Блокировка подключений конкретных устройств

[Мониторинг]

- Единый пакет инструментов «из коробки»
- Поддержка Zabbix 6.0 LTS
- Мониторинг С-Терра Шлюз DP

[Консоль]

- Расширенный набор команд CLI (VLAN, GRE, syslog, NTP, IPv6)
- Преднастроенный интерфейс управления
- SSH с аутентификацией администратора на RADIUS

Вопрос № 3

Есть ли законодательная регламентация использования софта на объекте КИИ? И в целом можно ли использовать западное ПО (ОС, СУБД, ПАК, SCADA) для обработки данных?

Импортозамещение

Запрет использования ПО и ПАК иностранного происхождения					
НПА	**Ссылка**	**Срок**	**Область действия**	**Предмет запрета**	**Суть запрета**
Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности КИИ РФ»	Пункт 1, подпункт «а»	с 31 марта 2022 г.	Заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с Федеральным законом от 18.07.2011 № 223-ФЗ	Иностранное ПО, в том числе в составе ПАК, с целью использования на ЗОКИИ, а также услуги, необходимых для использования этого ПО и/или ПАК	Запрет закупок без согласования с федеральным органом исполнительной власти, уполномоченным Правительством РФ
Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности КИИ РФ»	Пункт 1, подпункт «б»	с 1 января 2025 г.	Органы государственной власти, заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с Федеральным законом от 18.07.2011 № 223-ФЗ	Иностранное ПО	Запрет использования на ЗОКИИ
Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению ИБ РФ»	Пункт «б»	с 1 января 2025 г.	Федеральные органы исполнительной власти, высшие исполнительные органы государственной власти субъектов РФ, государственные фонды, государственные компании и иные организации, созданные на основании федеральных законов, стратегические предприятия, стратегические акционерные общества и системообразующие организации российской экономики, юридические лица, являющихся субъектами КИИ	Средства защиты информации	Запрет использования в случае, если странами происхождения являются недружественные иностранные государства
Указ Президента Российской Федерации от 13.06.2024 № 500 "О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"	Пункт 1, подпункт «в»	с 1 января 2025 г.	Федеральные органы исполнительной власти, высшие исполнительные органы государственной власти субъектов РФ, государственные фонды, государственные компании и иные организации, созданные на основании федеральных законов, стратегические предприятия, стратегические акционерные общества и системообразующие организации российской экономики, юридические лица, являющихся субъектами КИИ	Работы и услуги по обеспечению информационной безопасности	Запрет использования в случае, если страной происхождения организации является недружественное иностранное государство
Постановление Правительства РФ от 22.08.2022 № 1478 «Об утверждении требований к ПО, Правил согласования закупок иностранного ПО и услуг…»	Пункт «1» требований к ПО	с 1 января 2025 г.	Органы государственной власти, заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с Федеральным законом от 18.07.2011 № 223-ФЗ	Иностранное ПО, в том числе в составе ПАК, с целью использования на ЗОКИИ	Запрет использования в случае, если не включено в единый реестр российских программ для ЭВМ и БД или в единый реестр программ для ЭВМ и БД из государств - членов Евразийского экономического союза, за исключением РФ

Импортозамещение

Запрет использования ПО и ПАК иностранного происхождения					
НПА	**Ссылка**	**Срок**	**Область действия**	**Предмет запрета**	**Суть запрета**
Постановление Правительства РФ от 22.08.2022 № 1478 «Об утверждении требований к ПО, Правил согласования закупок иностранного ПО и услуг…»	Пункт «2» требований к ПО	с 1 января 2025 г.	Органы государственной власти, заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с Федеральным законом от 18.07.2011 № 223-ФЗ	ПО для обеспечения безопасности ЗОКИИ, для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ и/или обмена информацией о КИ	Запрет использования в случае, если не включено в единый реестр российских программ для ЭВМ и БД или в единый реестр программ для ЭВМ и БД из государств - членов Евразийского экономического союза, за исключением РФ, должны иметь соответсвующие сертификаты ФСТЭК и/или ФСБ России
Постановление Правительства РФ № 1912 «О порядке перехода субъектов КИИ РФ на преимущественное применение доверенных ПАК на принадлежащих им ЗО КИИ РФ»	Пункт «2»	с 1 сентября 2024 г.	Субъекты КИИ	ПАК, с целью использования на ЗОКИИ	Закупка и использование ПАК , приобретенных субъектами КИИ с 1 сентября и не являющихся доверенными ПАК (сведения о ПАК должны содержаться в едином реестре радиоэлектронной продукции, ПО в составе ПАК должно быть включено в реестр российских программ для ЭВМ и БД или в единый реестр программ для ЭВМ и БД из государств - членов Евразийского экономического союза, за исключением РФ, в случае реализации функций защиты информации должны быть соответсвующие сертификаты ФСТЭК и/или ФСБ России)
Постановление Правительства РФ № 1912 «О порядке перехода субъектов КИИ РФ на преимущественное применение доверенных ПАК на принадлежащих им ЗО КИИ РФ»	Пункт «2»	с 1 января 2030 г.	Субъекты КИИ	ПАК, с целью использования на ЗОКИИ	Использование ПАК не являющихся доверенными ПАК (сведения о ПАК должны содержаться в едином реестре радиоэлектронной продукции, ПО в составе ПАК должно быть включено в реестр российских программ для ЭВМ и БД или в единый реестр программ для ЭВМ и БД из государств - членов Евразийского

Импортозамещение

Постановление Правительства Российской Федерации от 22.08.2022 № 1478

"Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом "О закупках товаров, работ, услуг отдельными видами юридических лиц" (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, Правил согласования закупок иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования заказчиками, осуществляющими закупки в соответствии с Федеральным законом "О закупках товаров, работ, услуг отдельными видами юридических лиц" (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, а также закупок услуг, необходимых для использования этого программного обеспечения на таких объектах, и Правил перехода на преимущественное использование российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, органов государственной власти, заказчиков, осуществляющих закупки в соответствии с Федеральным законом "О закупках товаров, работ, услуг отдельными видами юридических лиц" (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации"

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

Планируется разработка документации на аппаратные платформы С-Терра и руководства по монтажу и размещение их на сайте?

с•терра®

… 4.1	4.2	4.3	5.0
С-Терра Шлюз	С-Терра СОВ	С-Терра Юнит	С-Терра Шлюз, Шлюз DP с КУ
С-Терра Вирт. Шлюз	С-Терра Шлюз DP	С-Терра Клиент А	С-Терра NGFW
С-Терра КП		С-Терра TLS Шлюз	С-Терра ГСУ
С-Терра Клиент		С-Терра TLS Клиент	

[Полезная информация в открытом доступе]

- Технические характеристики аппаратных платформ: https://www.s-terra.ru/catalog/ap.php

- Портал Документации с **Формулярами**, сценариями и руководствами: https://doc.s-terra.ru/

[Полезная информация в открытом доступе]

- Руководства по монтажу оборудования

Монтаж в стойку АП *LN-L* и *LN-XL*

1. Распакуйте коробку.
2. Извлеките рельсы и комплект крепежа из внутренней коробки.
3. Отсоедините внутренние направляющие (для крепления на АП) от внешних направляющих (для крепления в стойку):
   - Для этого выдвиньте выезжающие элементы до упора (Рисунок 1).

Рисунок 1

   - Сдвиньте ползунки белого цвета (Рисунок 2).

Рисунок 2

   - Отсоедините внутреннюю направляющую от внешней.
   - Выполните аналогичные действия для второй рельсы.

Внутренние и внешние направляющие раздельно (Рисунок 3).

- ⊕ Мониторинг
- ⊕ Инструкция по восстановлению и обновлению ПАК
- ⊕ Инструкции по деинсталляции Продукта С-Терра Шлюз
- ⊖ Приложение
  - ⊕ Монтаж АП на базе Lanner
  - ⊕ Соответствие интерфейсов АП на базе Lanner для С-Терра Шлюз
  - ⊕ Соответствие интерфейсов АП на базе Aquarius

[Сценарии использования в открытом доступе]

- Пошаговые сценарии применения продуктов (как это было у Cisco): на портале Документации

Начальные настройки

Дата и время на всех криптошлюзах и УЦ должны быть одинаковы, так как для аутентификации используются цифровые сертификаты, в которых зафиксированы дата и время начала их действия и окончания. Также одинаковые дата и время на всей инфраструктуре облегчают поиск неисправностей по лог-файлам.

1. Войдите в CLI разграничения доступа. Для этого, после появления сообщения:

```
S-Terra administrative console
```

введите логин и пароль для CLI разграничения доступа:

Пользователь и пароль по умолчанию: `administrator`, `s-terra`. Обязательно смените пароль для пользователя `administrator` при помощи команды `change user password`.

```
login as: administrator
administrator's password:
administrator@sterragate]
```

2. Установите правильный тип терминала (для `putty` тип терминала `xterm`) и требуемую ширину (для удобства работы), например:

```
administrator@sterragate] terminal terminal-type xterm
administrator@sterragate] terminal width 150
```

3. Установите нужную временную зону и правильные дату и время на криптошлюзе, используя консоль linux bash. Для этого выполните следующие команды.

3.1. Войдите в linux bash.

```
administrator@sterragate] system
Entering system shell...
```

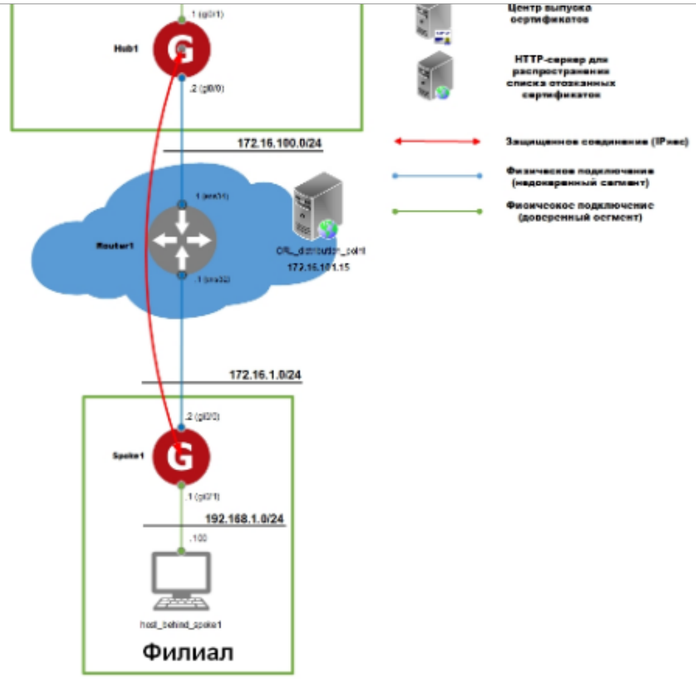


Рисунок 1. Схема взаимодействия

Общая логика работы

1. Размещение устройств.

1.1. В центральном офисе размещаются: центр выпуска сертификатов (Certification_authority), криптошлюз С-Терра Шлюз (Hub1) и персональный компьютер (host_behind_hub1).

Вопрос № 5

На какие НПА опираться при определении необходимого класса СКЗИ (КС1, КС2, КС3) на объектах КИИ, которые не являются ГИС и в которых не осуществляется обработка ПДн? Например, АСУ ТП

Допустимо ли применять меньший класс СКЗИ при условии реализации компенсирующих организационных мер (контроль доступа)?

Определение класса СКЗИ для ОКИИ (АСУ ТП)

Важно: на текущий момент **отсутствуют** НПА и методические документы, регламентирующие применение СКЗИ (в том числе определение необходимого класса СКЗИ) на объектах КИИ.

Применение СКЗИ на объектах КИИ необходимо в следующих случаях:

1) При наличие отраслевых требований по ИБ
2) В случае принятия соответствующего решения самим субъектом КИИ

Определение класса СКЗИ для ОКИИ (АСУ ТП)

Пример отраслевых требований от Минэнерго РФ

Министерство юстиции Российской Федерации
ЗАРЕГИСТРИРОВАНО
Регистрационный № 78165
от "16" мая 2024.

Министерство энергетики Российской Федерации
(Минэнерго России)

ПРИКАЗ

26 декабря 2023 г. № 1215

Москва

Об утверждении дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике

Криптографическая защита должна осуществляться с использованием средств криптографической защиты информации, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности[4].

Выбор класса используемых средств криптографической защиты информации необходимо проводить на основании модели угроз безопасности информации[5].

Определение класса СКЗИ для ОКИИ (АСУ ТП)

Ответ ФСБ России на официальный запрос:

Обеспечение безопасности объектов КИИ относится к компетенции ФСТЭК России.

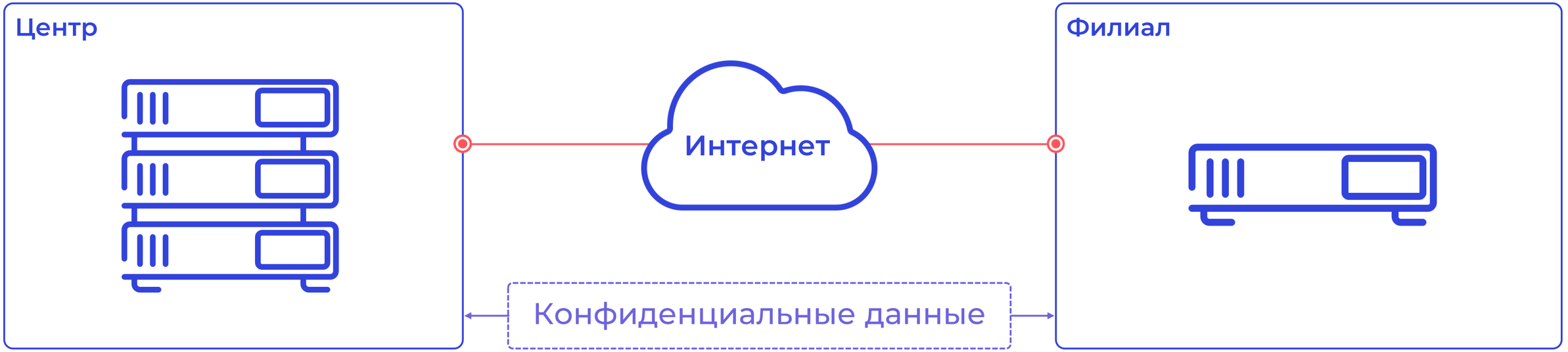
Для определения класса СКЗИ, применяемых на объектах КИИ рекомендуем руководствоваться положениями Приказа ФСБ России от 18 марта 2025 года № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств».

Определение класса СКЗИ для ОКИИ (АСУ ТП)

Подход по определению класса СКЗИ для ОКИИ:

1) При разработке модели угроз определяем модель нарушителя, его потенциал и возможности, а также акутальные угрозы (в том числе, связанные с каналами связи)
2) В проектной документации на создание системы обеспечения ИБ определяем угрозы, нейтрализация которых осуществляется с помощью СКЗИ
3) В проектной документации определяем необходимый класс СКЗИ, руководствуясь результатами моделирования угроз и приказом ФСБ России от 18 марта 2025 г. N 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств»

ДЛЯ ЧЕГО НУЖНЫ СКЗИ С-ТЕРРА?



Объекты КИИ

187-ФЗ от 26.07.2017
Приказ **ФСТЭК России** №239, №235. Приказ **ФСБ России** о ГОССОПКА

Импортозамещение

Указ **Президента РФ** №250
Постановление **Правительства РФ** №1912

Персональные данные

152-ФЗ от 27.07.2006
Приказ **ФСТЭК России** №17, 21. Приказ **ФСБ России** №378

Энергетика

Приказ **Министерства Энергетики** №1215 от 16.05.2024

Вопрос № 6

С-Терра Шлюз ST (КС1, КС2, КС3)
В версии 4.3, при добавлении параметра distance (метрика) к маршруту, используя команду ip route данной параметр не применяется/игнорируется. ТП ответила, что в текущей версии данный параметр не поддерживается.

Будет ли поддерживаться данный функционал в будущих версиях?

ПРИМЕР » Резервирование

Задайте маршрут по умолчанию через LAN интерфейс с метрикой 100:
Hub1-n1(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.20 *100*
(Чем меньше число, тем выше приоритет маршрута)

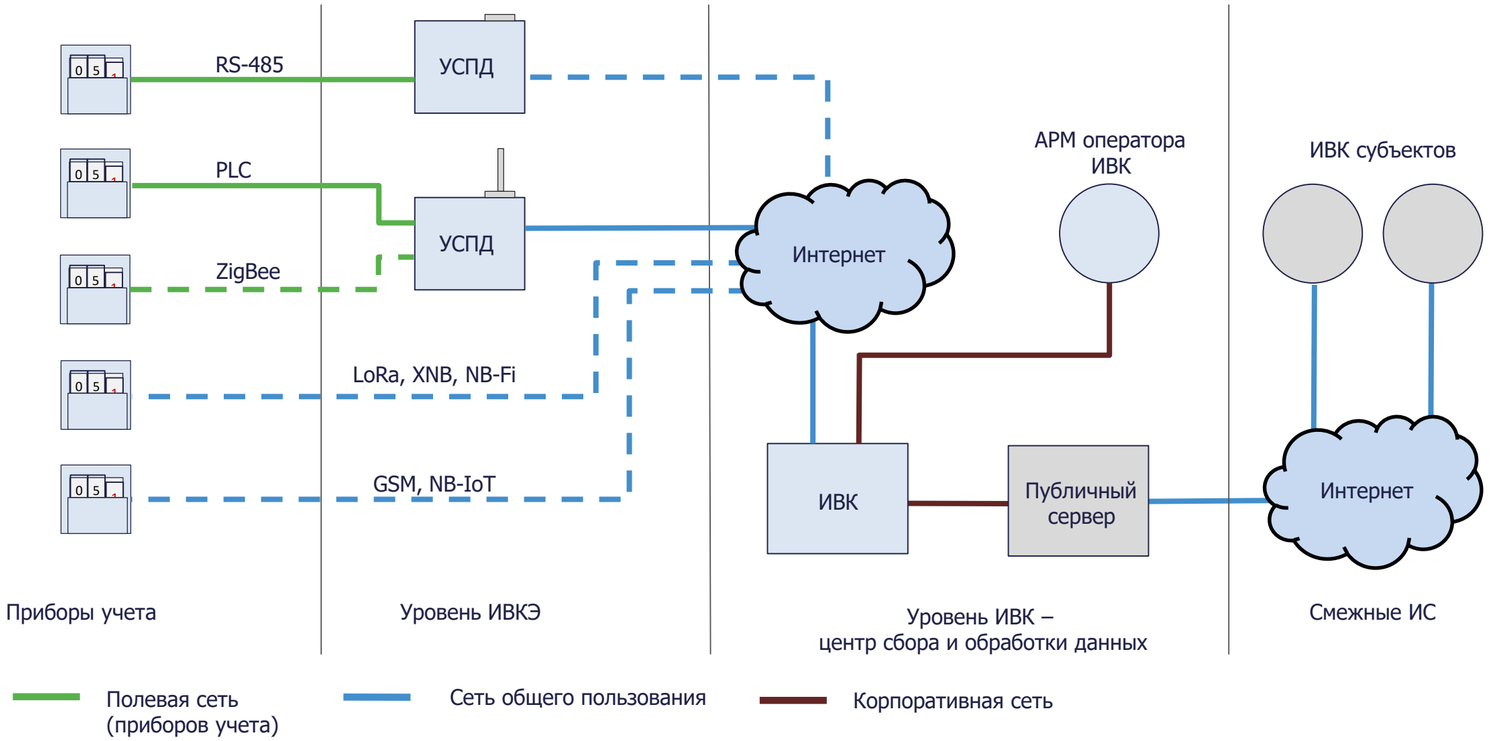
При помощи сервиса MultiWAN:
iface_name: eth0
prio: 300
(Канал с большим значением prio будет считаться приоритетным)

Вопрос № 7

Как категорировать информационно-вычислительную систему (ИВС) верхнего уровня автоматизированной системы учета электроэнергии в распределительных сетях? Рассматривать ее как АСУ, целиком с счетчиками, поскольку есть управляемая нагрузка в виде счетчиков (ПУЭ), или считать, что в ПУЭ не протекают критические процессы и рассматривать только ИВС?

Назначение системы - автоматизация функций сбора, хранения, анализ и передача в смежные информационные системы данных с приборов учета электроэнергии

Категорирование АСКУЭ

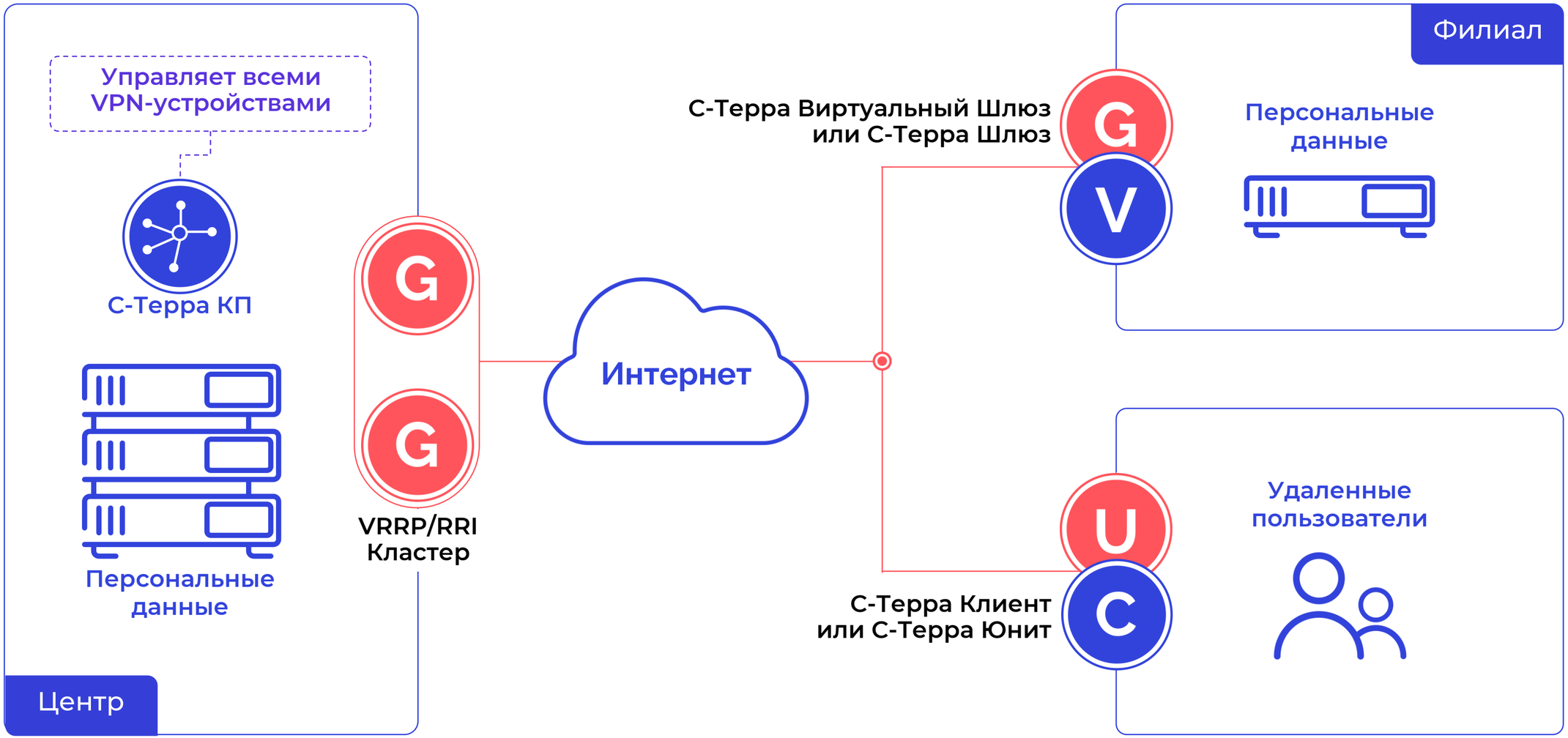


Вопрос № 8

Сетевая безопасность и защита каналов связи на значимых объектах КИИ (например, ИС) в условиях территориальной рассредоточенности (разные районы города) рабочих мест, с которых осуществляется подключение

ЗАЩИТА КОРПОРАТИВНОЙ СЕТИ – РАСПРЕДЕЛЕННЫЕ СЕТИ

ПРИМЕР » Отказоустойчивость в центре, связь с филиалами и удаленным офисом



Рекомендуем к просмотру

Запись вебинара
«Удаленный доступ к критической инфраструктуре:
как совместить удобство и безопасность»:

Вопрос № 9

Требуется пояснить кто определяет ОКИИ - комиссия или ФЗ:

- **в ФЗ № 187 статья 2. п.7 определяет ОКИИ - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры**

- **в Постановлении Правительства РФ № 127 в правилах категорирования ОККИ в п.14 сказано, что комиссия по категорированию определяет процессы, указанные в пункте 3 настоящих правил, а именно - категорированию подлежат ОКИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и иные процессы в рамках выполнения функций или осуществления видов деятельности субъектов КИИ в областях, установленных пунктом 8 статьи 2 ФЗ "О безопасности КИИ РФ".**

Вопрос № 10

На что стоит обратить особое внимание при проектировании системы обеспечения безопасности объектов КИИ?

Проектная документация

Том проектной документации в составе:

- ✓ Пояснительная записка в объеме:
  - определение объектов защиты;
  - определение политики управления доступом;
  - определение организационных и технических мер защиты;
  - определение видов и типов средств защиты информации;
  - определение архитектуры подсистемы безопасности.
- ✓ Спецификация оборудования и ПО подсистемы ИБ.
- ✓ Ведомость объемов работ.
- ✓ Графическая часть:
  - схема комплекса технических средств ОКИИ с указанием средств защиты информации;
  - схема размещения оборудования;
  - схема электропитания.

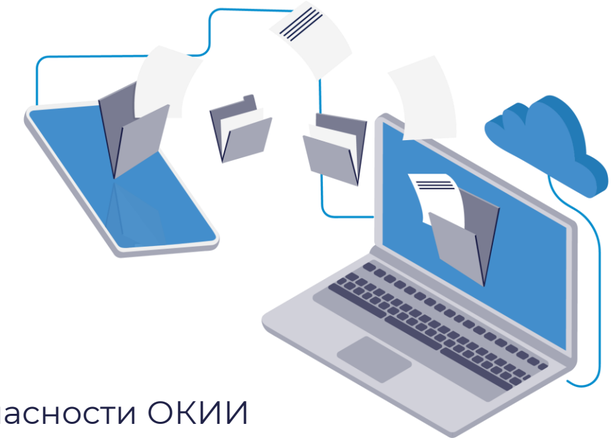
Состав ПД определяется и согласовывается с Заказчиком на этапе разработки ТЗ на создание ОКИИ и (или) ТЗ на создание системы защиты

Рабочая (эксплуатационная) документация

Том рабочей документации в составе:

- ✓ Основной комплект рабочих чертежей в объеме:
  - Схема структурная комплекса технических средств подсистемы информационной безопасности ОКИИ;
  - План размещения шкафа ИБ;
  - Схема электропитания шкафа ИБ;
  - Схема интерфейсных соединений;.
  - Кабельный журнал;
  - Спецификация оборудования, изделий и материалов.
- ✓ Параметрирование СЗИ:
  - Настройка средств защиты информации.
  - Настройка системного ПО.
  - План распределения IP-адресов.
- ✓ Документация по испытанию подсистемы ИБ:
  - Программа и методика предварительных испытаний подсистемы информационной безопасности ОКИИ
  - Программа опытной эксплуатации подсистемы информационной безопасности ОКИИ
  - Программа и методика приемочных испытаний подсистемы информационной безопасности ОКИИ
- ✓ Задание заводу на изготовление шкафа ИБ: схема электрических соединений, перечень элементов, чертеж общего вида

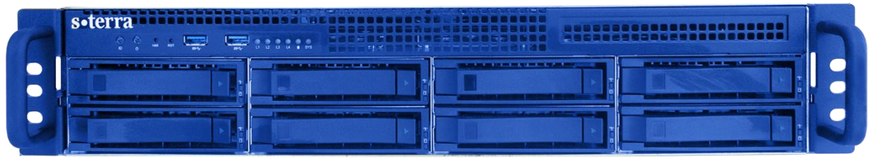
Состав РД определяется и согласовывается с Заказчиком на этапе разработки ТЗ на создание ОКИИ и (или) ТЗ на создание системы защиты

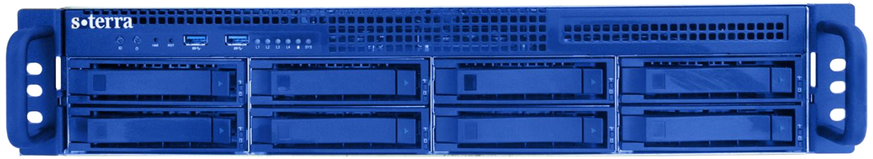


КРИТЕРИИ ВЫБОРА ОБОРУДОВАНИЯ

КАК МОЖНО СОСТАВИТЬ СПЕЦИФИКАЦИЮ ОБОРУДОВАНИЯ

С-Терра ГСУ/ КП — система централизованного управления





С-Терра Шлюз 3000НЕ — до **3 500** Мбит/с
С-Терра Шлюз 7000НЕ — до **4 000** Мбит/с

С-Терра Шлюз 100
до **200** Мбит/с

С-Терра Юнит
до **10** Мбит/с

С-Терра Виртуальный Шлюз
до **2 000** Мбит/с

С-Терра Клиент
защита **удаленного** доступа

Вопрос № 11

Каковы требования к образованию (переподготовке) специалистов по защите информации в субъекте КИИ без значимых объектов КИИ/ со значимыми объектами КИИ, в том числе согласованность программы со ФСТЭК, продолжительность, частота переобучения?

Требования к силам обеспечения безопасности ЗОКИИ

Должность	Требования к образованию	Требованию к стажу	Требования к повышению квалификации	Основание
Руководитель структурного подразделения по ИБ	Высшее профессиональное образование в области ИБ либо иное высшее образование и прохождение профессиональной переподготовки по направлению ИБ	Опыт работы в сфере ИБ не менее 3 лет	Повышение квалификации по профильному направлению не реже 1 раза в 3 года	Приказ ФСТЭК России от 21.12.20217 г. № 235
Сотрудники структурного подразделения по ИБ	Высшее или среднее профессиональное образование по направлению ИБ либо высшее образование и повышение квалификации по направлению ИБ	-	Повышение квалификации по профильному направлению не реже 1 раза в 3 года	Приказ ФСТЭК России от 21.12.20217 г. № 235
Заместитель руководителя субъекта КИИ, ответственный за обеспечение ИБ	Высшее профессиональное образование в области ИБ (не ниже уровня специалитета, магистратуры) либо иное высшее образование и прохождение профессиональной переподготовки по направлению ИБ	-	-	Постановление Правительства РФ от 15.07.2022 г. № 1272

Мы поможем Вам защитить данные и выполнить требования НПА

Компания КСБ-СОФТ оказывает полный комплекс услуг по защите объектов КИИ

Безопасность объектов КИИ

Выявление и категорирование объектов КИИ, разработка и внедрение комплексного решения по обеспечению безопасности значимых объектов КИИ, организация взаимодействия с центром ГосСОПКА, анализ уязвимостей и пентест

Импортозамещение

Решение задач импортозамещения в соответствии со стратегией развития информационного общества в Российской Федерации

SOCRAT - центр мониторинга и реагирования на инциденты информационной безопасности

Мониторинг и предотвращение атак на начальных стадиях, либо выявление следов проникновения

Оценка показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры

Выполнение работ по новой методике ФСТЭК России от 02.05.2024 г.

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

Телеграм-канал
«Мнение интегратора»

Задайте свой
вопрос для разбора
на следующем вебинаре

ПИШИТЕ НАМ И ВСТУПАЙТЕ В СООБЩЕСТВО ИНЖЕНЕРОВ

[Официальный канал]

- RELEASE NOTES
- СЦЕНАРИИ ДЛЯ НОВОЙ ВЕРСИИ
- ДЕМОНСТРАЦИОННЫЕ ВЕРСИИ И ЛИЦЕНЗИИ
- АНОНСЫ НАШИХ МЕРОПРИЯТИЙ

[Неофициальный инженерный чат]

- ЖИВОЕ СООБЩЕСТВО ИНЖЕНЕРОВ
- ВОПРОСЫ ПО ТЕХНИКЕ
- СОТРУДНИКИ С-ТЕРРА В ЧАТЕ

presale@s-terra.ru

sales@s-terra.ru

+7 (499) 940-90-01