КСБ-СОФТ

КОД безопасности

Ответы на насущные вопросы по информационной безопасности объектов КИИ. Часть 3

Спикеры:

- **Шляпкин Максим –** руководитель отдела защиты объектов КИИ и АСУ ТП, КСБ-СОФТ
- **Коростелев Павел** - руководитель отдела продвижения продуктов «Кода Безопасности»

Модератор:

- **Ильин Александр –** 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

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»

План вебинара

- нюансы реализации мер 239-го приказа ФСТЭК России при защите объектов КИИ
- анализ функционирования системы безопасности и оценка защищенности объектов КИИ
- регламентация технических мер при создании системы безопасности объектов объектов КИИ
- сетевая безопасность и решение проблем импортозамещения устройств класса NGFW/UTM/FW

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

При реализации мер 239 приказа ФСТЭК каким образом можно исключить базовую меру?

Выбор мер по обеспечению безопасности ЗОКИИ

1 Определение базового набора мер по обеспечению безопасности ЗОКИИ

Определяется на основании присвоенной категории значимости ЗОКИИ

2 **Адаптация базового набора мер по обеспечению безопасности ЗОКИИ**

Подлежит адаптации в соответствии с:

- **угрозами безопасности информации;**
- **применяемыми информационными технологиями;**
- **особенностями функционирования ЗОКИИ**

3 Дополнение адаптированного набора мер по обеспечению безопасности ЗОКИИ мерами, установленными иными НПА в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации и защиты информации

Дополнение адаптированного набора мер проводится в случае, если в отношении ЗОКИИ установлены требования о защите информации, содержащейся в ГИС, требования к защите ПДн, требования к криптографической защите информации или иные требования в области защиты информации и обеспечения КИИ

Вопрос № 2

Есть ли у Кода Безопасности решения для защиты беспроводных технологий?

Вопрос № 3

Как реализовать межсетевое экранирование в виртуальной среде?

Вопрос № 4

Под категорию попали автономные станки с ЧПУ иностранного производства. В соответствии с ПП 1912, необходимо произвести импортозамещение до конца 2030г. Но аналогов подобных станков в РФ нет и вряд ли будут. Как быть в подобной ситуации в вопросе импортозамещения?

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

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"

Вопрос № 5

Согласно п.37 приказа ФСТЭК №235 в рамках совершенствования безопасности ЗОКИИ должен проводиться анализ функционирования системы безопасности. Каким образом этот анализ выполняется и чем подтверждается его выполнение, какая периодичность данного мероприятия? (для контроля состояния безопасности, например, в п.35 указан срок 3 года)

Анализ функционирования системы безопасности и состояния безопасности ЗОКИИ

Кем осуществляется?

Структурным подразделением по безопасности, специалистами по безопасности с участием подразделений (работников), эксплуатирующих ЗОКИИ, и подразделений (работников), обеспечивающих функционирование ЗОКИИ

Что на выходе?

Предложения по развитию системы безопасности и меры по совершенствованию безопасности ЗОКИИ, которые предоставляются руководителю субъекта КИИ

Дальнейшие действия?

Формирование предложений по совершенствованию безопасности ЗОКИИ включаются в ежегодный план мероприятий по обеспечению безопасности ЗОКИИ

Анализ функционирования системы безопасности и состояния безопасности ЗОКИИ

Примеры возможных работ в рамках анализа функционирования системы и состояния безопасности ЗОКИИ:

- оценка показателя состояния технической защиты информации по Методике ФСТЭК России от 02 мая 2024 г.;
- аудит на соответствие требованиям НПА по ИБ КИИ, инструментальный аудит (внутренний либо внешний);
- анализ уязвимостей, пентест ЗОКИИ

Примеры отчетных документов:

- акт оценки показателя защищенности ЗОКИИ + план реализации мероприятий по повышению уровня защищенности;
- отчет о проведении аудита/анализа уязвимостей/пентеста с рекомендациями по совершенствованию системы безопасности ЗОКИИ;
- перечень предложений по совершенствованию безопасности ЗОКИИ;
- скорректированный ежегодный план мероприятий по обеспечению безопасности ЗОКИИ

Периодичность проведения анализа функционирования системы безопасности и состояния безопасности ЗОКИИ в НПА не регламентирована.

Вопрос № 6

Есть ли минимальные требования к NGFW Континент 4, который в одном устройстве совмещает функции межсетевого экранирования, системы обнаружения вторжений и шифрования трафика, особенно с учетом использования кластера?

Вопрос № 7

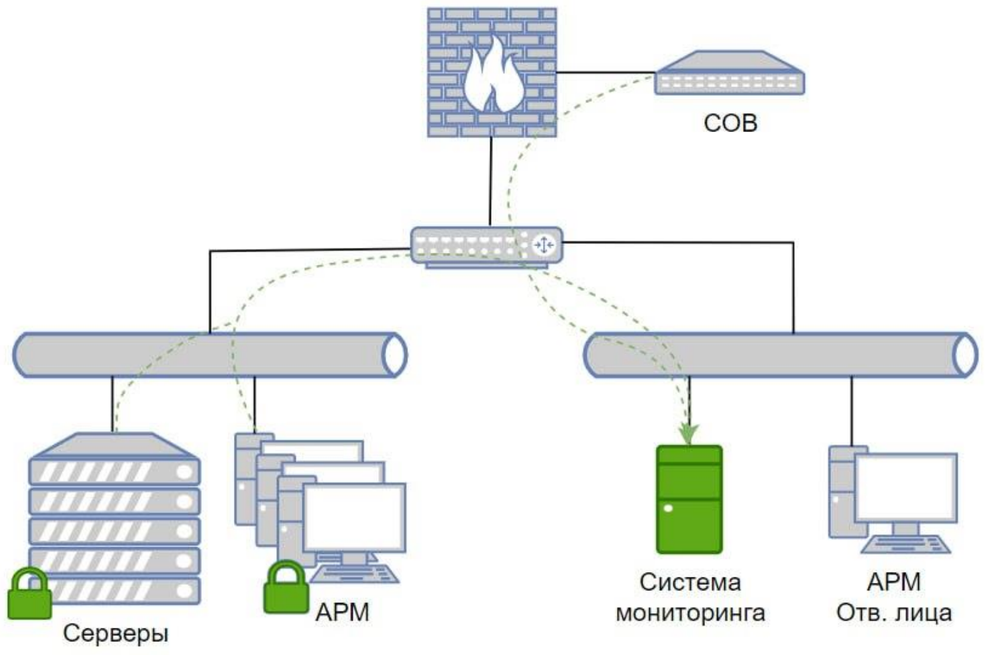
Как реализован СОВ в NGFW Континент 4? Мониторинг только проходящего через него трафика? Или есть возможность анализа трафика с подключенных к NGFW SPAN-портов коммутатора? В случае мониторинга проходящего трафика не вносится ли задержка в передачу трафика?

Вопрос № 8

Хотелось бы рассмотреть 239 приказ ФСТЭК в части требований по мониторингу безопасности, имеется ли ввиду под этим SIEM?

Мониторинг безопасности

V. Аудит безопасности (АУД)				
АУД.0	Регламентация правил и процедур аудита безопасности	+	+	+
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.2	Анализ уязвимостей и их устранение	+	+	+
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	+	+
АУД.4	Регистрация событий безопасности	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.6	Защита информации о событиях безопасности	+	+	+
АУД.7	Мониторинг безопасности	+	+	+
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	+	+
АУД.9	Анализ действий отдельных пользователей			+
АУД.10	Проведение внутренних аудитов	+	+	+
АУД.11	Проведение внешних аудитов			



Мониторинг безопасности. Возможности MaxPatrol SIEM

MaxPatrol SIEM предоставляет следующие основные возможности:

- Инвентаризация активов. Система регулярно собирает данные о сетевых узлах и связях между ними.
- Сбор данных о событиях. В качестве источника событий может выступать любое поддерживаемое оборудование или ПО.
- Анализ событий для выявления инцидентов ИБ. Набор специальных правил, на основе которых выполняется анализ, постоянно пополняется экспертами Positive Technologies.
- Управление инцидентами ИБ. Система помогает организовать работу по расследованию инцидентов информационной безопасности и устранению их последствий.
- Визуализация данных. Сводная информация об активах, событиях и инцидентах отображается в веб-интерфейсе системы в виде диаграмм и таблиц.

MaxPatrol SIEM предоставляет также дополнительные возможности:

- Пакеты экспертизы. Использование базы знаний, разработанной экспертами Positive Technologies. База содержит данные о самых современных тактиках и техниках хакерских атак и помогает выявлять даже сложные нетиповые атаки.
- Автоматизация работы с активами. Система может автоматически устанавливать значимость активов и сроки актуальности данных об активах, полученных в результате сканирования IT-инфраструктуры.
- Репутационные списки. Актуальная информация о вредоносных IP-адресах и хеш-суммах опасных файлов используется для предотвращения инцидентов.
- Повторная проверка событий. Ретроспективная корреляция полученных ранее событий после добавления новых правил или обновления данных табличных списков; ретроспективный поиск индикаторов компрометации.
- Отправка уведомлений. Оповещение операторов об изменениях в IT-инфраструктуре предприятия, о работе задач сбора данных, собираемых событиях, а также о выявляемых инцидентах ИБ.
- Интеграция с PT NAD. Регистрация инцидентов на основе сессий и атак.

Информация взята с портала: https://help.ptsecurity.com/ru-RU/projects/siem/latest/help/93816075

Вопрос № 9

a) **Хотелось бы обсудить Методику оценки КИИ от 2 мая 2024 г. Планируется ли такое мероприятие?**

b) **ФСТЭК утверждены методические рекомендации по оценке показателя технической защиты ЗОКИИ, это необходимо проводить раз в 6 месяцев. Если ЗОКИИ сейчас модернизируется, то могу ли я учитывать при оценке то, что заложено в проект модернизации, но еще не реализовано?**

Показатель защищенности (Кзи)

В качестве показателя, характеризующего текущее состояние защиты информации (обеспечения безопасности объектов КИИ) в организации, в методике используется **показатель текущего состояния защищенности Кзи**, который характеризует степень достижения организацией **минимально необходимого уровня защиты информации** от типовых актуальных угроз безопасности информации ИС, АСУ, ИТКС и иных объектов информатизации.

Для оценки КЗИ определяются значения частных показателей безопасности kji.

Частные показатели безопасности характеризуют реализацию в организации отдельных мер по защите информации. Каждому частному показателю в методике присвоен определенный «вес» и все они поделены на следующие группы:

- организация и управление;
- защита пользователей;
- защита информационных систем;
- мониторинг информационной безопасности и реагирование.

Частные показатели

Номер группы показателей (j)	Наименование групп показателей	Номер (i) и наименование показателя безопасности	Значение частного показателя (k_{ji})	Значение весового коэффициент группы показателей (R_j)
1.	Организация и управление	1. На заместителя руководителя органа (организации) возложены[3] полномочия ответственного лица за обеспечение информационной безопасности органа (организации) и определены его обязанности	0,30	0,10
		2. Определены функции (обязанности) структурного подразделения (или отдельных работников), ответственного за обеспечение информационной безопасности органа (организации)	0,40	
		3. К подрядным организациям, имеющим доступ к информационным системам с привилегированными правами, в договорах установлены требования о реализации мер по защите от угроз через информационную инфраструктуру подрядчика[4]	0,30	

Частные показатели

Номер группы показателей (j)	Наименование групп показателей	Номер (i) и наименование показателя безопасности	Значение частного показателя (k_{ji})	Значение весового коэффициент группы показателей (R_j)
2.	Защита пользователей	1. Отсутствуют учетные записи с паролем, сложность которого не соответствует установленным требованиям к парольной политике. В случае отсутствия технической возможности обеспечения требуемой сложности паролей реализованы компенсирующие меры	0,30	0,25
		2. Реализована многофакторная аутентификация привилегированных пользователей (при аутентификации не менее 50% администраторов, разработчиков или иных привилегированных пользователей используется второй фактор)[3]	0,30	
		3. Отсутствуют учетные записи разработчиков и сервисные учетные записи с паролями, установленными ими по умолчанию	0,20	
		4. Отсутствуют активные учетные записи работников органа (организации) и работников, привлекаемых на договорной основе, с которыми прекращены трудовые или иные отношения	0,20	

Частные показатели

Номер группы показателей (j)	**Наименование групп показателей**	Номер (i) и наименование показателя безопасности	Значение частного показателя (k_{ji})	Значение весового коэффициент группы показателей **(R_j)**
3.	Защита информационных систем	1. На сетевом периметре информационных систем установлены межсетевые экраны уровня L3/L4 (доступ к 100% интерфейсов, доступных из сети Интернет[1], контролируется межсетевыми экранами уровня L3/L4)	0,20	0,35
		2. На устройствах и интерфейсах, доступных из сети Интернет, отсутствуют уязвимости критического уровня опасности с датой публикации обновлений (компенсирующих мер по устранению) в банке данных угроз ФСТЭК России, на официальных сайтах разработчиков, иных открытых источниках более 30 дней или в отношении таких уязвимостей реализованы компенсирующие меры	0,20	
		3. На пользовательских устройствах и серверах отсутствуют уязвимости критического уровня с датой публикации обновления (компенсирующих мер по устранению) более 90 дней (не менее 90% устройств и серверов) или в отношении таких уязвимостей реализованы компенсирующие меры	0,10	
		4. Обеспечен документальный или автоматизированный учет пользовательских устройств, серверов и сетевых устройств (не менее 80% устройств и серверов учтено в документах (ведомостях, паспортах, эксплуатационной документации) или в автоматизированных системах (CMDB))	0,10	
		5. Обеспечена проверка вложений в электронных письмах электронной почты[2] на наличие вредоносного программного обеспечения (проверяются вложения не менее чем на 80% пользовательских устройств)	0,15	
		6. Обеспечено централизованное управление средствами антивирусной защиты[3] (не менее чем 80% пользовательских устройств[4] контролируются средствами антивирусной защиты с централизованным управлением). При этом обеспечены контроль и установка обновлений баз данных признаков вредоносного программного обеспечения не реже чем 1 раз в месяц	0,15	
		7. Реализована очистка входящего из сети Интернет сетевого трафика от аномалий на уровне[5] L3/L4 (заключен договор с провайдером)	0,10	

Частные показатели

Номер группы показателей (j)	**Наименование групп показателей**	Номер (i) и наименование показателя безопасности	Значение частного показателя (k_{ji})	Значение весового коэффициент группы показателей **(R_j)**
4.	Мониторинг информационной безопасности и реагирование	1. Реализован централизованный сбор событий безопасности и оповещение о неудачных попытках входа для привилегированных учетных записей	0,40	0,30
		2. Реализован централизованный сбор и анализ событий безопасности на всех устройствах, взаимодействующих с сетью Интернет	0,35	
		3. Утвержден документ, определяющий порядок реагирования на компьютерные инциденты	0,25	

Расчет показателя защищенности

$$K_{ЗИ}=(k_{11}+k_{12}+k_{13})R_1+(k_{21}+k_{22}+...+k_{2i})R_2+(k_{31}+k_{32}+...+k_{3i})R_3+(k_{41}+k_{42}+...+k_{4i})R_4,$$

Где:

R_j — весовой коэффициент
j — й группы частных показателей безопасности

Значение $K_{ЗИ}$	Текущее состояние защиты информации (обеспечения безопасности объектов КИИ)
$K_{ЗИ}=1$	Обеспечивается минимальный уровень защиты от типовых актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как минимальный базовый («зеленый»)
$0,75<K_{ЗИ}<1$	Минимальный уровень защиты от актуальных угроз безопасности информации не обеспечивается, имеются предпосылки реализации актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как низкий («оранжевый»)
$K_{ЗИ}\leq 0,75$	Минимальный уровень защиты от актуальных угроз безопасности информации не обеспечивается, имеется реальная возможность реализации актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как критический («красный»)

Оценка показателя состояния технической защиты информации и обеспечения безопасности ЗОКИИ

Работы	Отчётные документы
Экспертный аудит для сбора исходных данных, необходимых для оценки показателя защищенности	Отчет о проведении аудита с результатами проведения опроса (интервьюирования) работников
Анализ уязвимостей устройств и интерфейсов, доступных из сети Интернет, а также пользовательских устройств и серверов	Отчет об анализе уязвимостей
Регламентация оценки показателя технической защищенности	Регламент оценки показателя технической защищенности
Проведение оценки показателя защищенности	Акт оценки показателя защищенности
Планирование работ по защите информации	План реализации мероприятий по повышению уровня защищенности

Вопрос № 10

a) **Какие документы должны быть в организации при ЗОКИИ? (не для категорирования, а при уже полученной категории). Такие как план мероприятий, регламент реагирования на инциденты, модель угроз и пр. Есть ли исчерпывающий перечень?**

b) **При регламентации технических мер при создании системы безопасности ОКИИ какие документы необходимо разработать и что в них указать?**

Этап 1. ОРД и документация по установлению требований

- Приказ о комиссии по категорированию ОКИИ
- Приказ об утверждении Положения о комиссии по категорированию ОКИИ
- Приказ о структурном подразделении, осуществляющем функции по обеспечению информационной безопасности
- Приказ об ответственном за обеспечение информационной безопасности
- Приказ о сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них
- План мероприятий по реализации требований Федерального закона № 187-ФЗ
- План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак
- Положение о внешнем взаимодействии при обеспечении безопасности КИИ
- Акт категорирования ОКИИ
- Сведения о результатах присвоения ОКИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий
- Модель угроз безопасности информации ОКИИ
- Частное техническое задание на создание подсистемы безопасности ОКИИ

Этап 2. Проектная документация

Том проектной документации в составе:

- ✓ Пояснительная записка в объеме:
  - пределение 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.

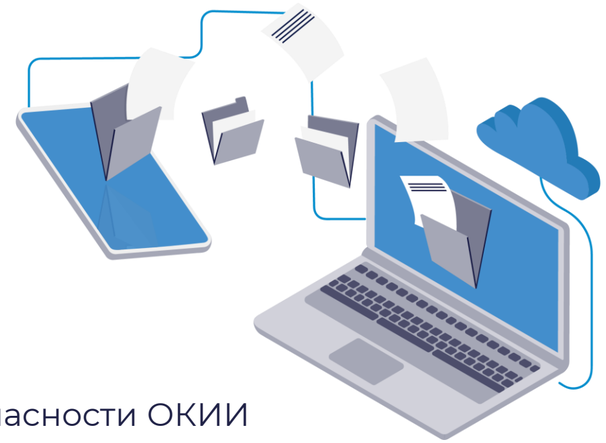
Состав ПД определяется и согласовывается с Заказчиком на этапе разработки ТЗ на создание ОКИИ и (или) ТЗ на создание системы защиты

Этап 3. 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



Этап 4. Организационно-распорядительная документация

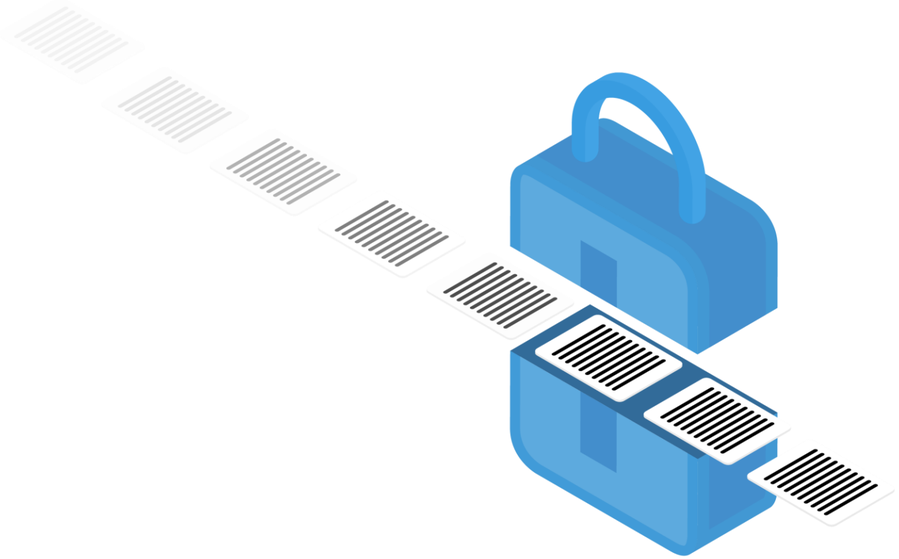
- Приказ об ответственном за обеспечение безопасности значимых объектов критической информационной инфраструктуры
- Приказ о сотрудниках, которым разрешены действия по внесению изменений в конфигурацию значимого объекта КИИ
- Приказ о силах обеспечения безопасности значимых объектов критической информационной инфраструктуры (при наличии значимых объектов КИИ)
- Приказ о назначении администратора безопасности объектов КИИ (при наличии значимых объектов КИИ)
- Приказ об ответственном за планирование и контроль мероприятий по обеспечению информационной безопасности (при наличии значимых объектов КИИ)
- Приказ об ответственном за управление (администрирование) подсистемой безопасности (при наличии значимых объектов КИИ)
- Приказ о контролируемых зонах

Этап 4. Организационно-распорядительная документация

- Регламент идентификации и аутентификации в объектах КИИ
- Регламент управления доступом в объектах КИИ
- Регламент ограничения программной среды в объектах КИИ
- Регламент защиты машинных носителей информации в объектах КИИ
- Регламент аудита безопасности объектов КИИ
- Регламент антивирусной защиты в объектах КИИ
- Регламент предотвращения вторжений (компьютерных атак) в объектах КИИ
- Регламент обеспечения целостности объектов КИИ
- Регламент обеспечения доступности объектов КИИ
- Регламент защиты технических средств и систем объектов КИИ
- Регламент защиты информационной (автоматизированной) системы и ее компонентов
- Регламент обновления программного обеспечения объектов КИИ
- Регламент действий сотрудников при возникновении нештатных ситуаций на объектах КИИ
- Регламент информирования и обучению персонала объектов КИИ

Что может дополнительно запросить регулятор у субъектов КИИ?

- ✓ Паспорт системы безопасности ЗО КИИ;
- ✓ Результаты оценки состояния технической защиты информации и обеспечения безопасности объектов информатизации:
  - Регламент оценки показателя КЗИ
  - Акт оценки показателя состояния технической защиты информации и обеспечения безопасности объектов информатизации
  - План реализации мероприятий по повышению уровня защищенности
- ✓ Приказ по утверждению Плана мероприятий по устранению уязвимостей
- ✓ Приказ по утверждению Регламента по анализу и установке обновлений безопасности
- ✓ Приказ по утверждению Регламента по выявлению, анализу и устранению критичных уязвимостей
- ✓ Результататы мероприятий по реагированию на компьютерный инцидент и принятию мер по ликвидации последствий компьютерных атак



Вопрос № 11

Есть способ настройки Континента 4 на объекте без удаленного ЦУСа?

Вопрос № 12

Для настройки ЦУС и МЭ требуется еще дополнительная установка специального ПО "ПУ ЦУС", которое работает под управлением Windows. Когда планируется переход на Linux?

Вопрос № 13

Вопрос по Континент 4.
МЭ цепляется к ЦУСу, если ЦУС вышел из строя, то при установке нового ЦУСа, настройки МЭ сбрасываются в 0, как это решить?
Есть ли решения без сбрасывания на живой системе?

Вопрос № 14

- **Когда ожидается получение сертификата на СКЗИ ФСБ России на Континент 4?**
- **Потребуется ли дополнительная прошивка или замена платформы после получения сертификата?**
- **Можно ли будет обновиться с версии 3.9?**

Вопрос № 15

**Средства ИБ для КИИ нередко значительно дороже,
это наценка за лицензию или за расширенные возможности?**

СЗИ для АСУ ТП. Особенности

Специфика АСУ ТП

Сложность интеграции

Технические характеристики

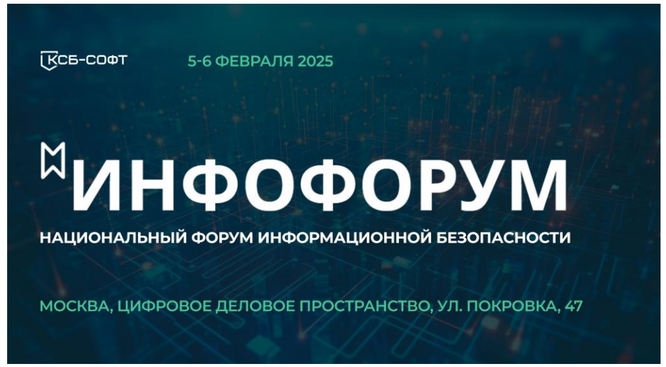
Требования регуляторов

Обучение и тех. поддержка

Ограниченность рынка

Приглашаем вас посетить наши стенды!

5-6 февраля, Москва



Сессия 1: Киберинциденты-2024/25 и Защита критической информационной инфраструктуры: новые решения, время работы сессии 13:00-18:00

Анна Павлова: "Метод SOCRATa"

11-13 февраля, Москва

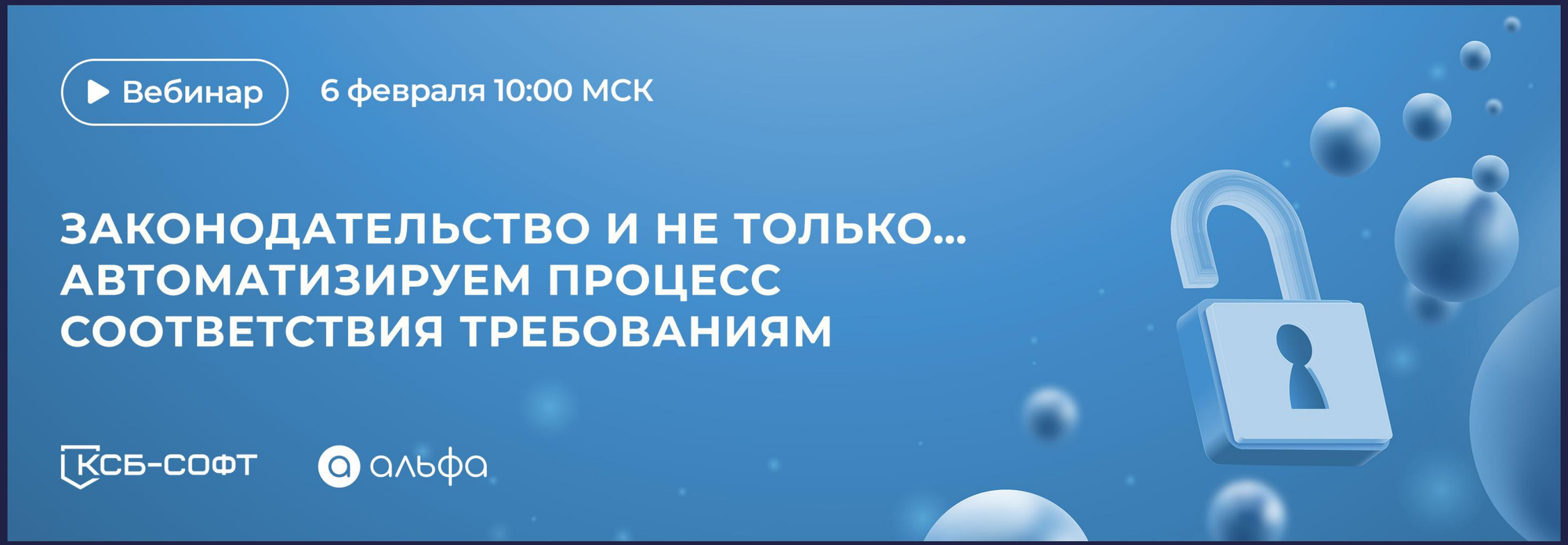
Секция: Комплексный подход к кибербезопасности. Защита АСУ ТП. Безопасность КИИ – **11 февраля**

Татьяна Егорова: «Проектирование комплексных систем ИБ ОКИИ: взгляд со стороны интегратора»

Секция: Подходы и инструменты управления процессом разработки безопасного программного обеспечения. От сертификации СЗИ к сертификации РБПО – **13 февраля**

Степан Харитонов: «Путешествие к безопасному ПО: идти медленно одному или далеко вдвоем?»

Приглашаем вас на вебинар!



Подробно разберем:

- Что такое эффективный compliance?
- Чему соответствовать и с чего начать?
- АльфаДок. Как работает, интеграционные возможности, основные изменения в продукте и планы на будущее.
- АльфаКрипто. Автоматизация учета СКЗИ и взаимодействия ОКЗ и ОКИ.
- АльфаКоннект. Автоматизация регламентации и контроля подключения пользователей к информационным системам.
- Идентификацию и аутентификацию с помощью Альфа-ID.

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