Информзащита
Системный интегратор

Автоматизированное реагирование при защите критических объектов

www.infosec.ru

Группа компаний «Информзащита»

АО НИП «Информзащита»

Специализируется в

обеспечения безопасности информационных систем

28 лет

является **лидером** российского рынка ИБ

Центры компетенций НИП Информзащита

Что требует учитывать комплексная безопасность промышленного предприятия РФ сегодня

Целевая Система Комплексной безопасности - интегрированная система, включающая все элементы безопасности (в том числе, кибербезопасность) объекта, объединенные в общую информационную среду.

Автоматизированное реагирование на наиболее разрушительные угрозы – требование сегодняшнего дня.

Защита воздушной полусферы

Кибербезопасность

Средства охраны

Все виды функциональной безопасности

Защищенность бизнес и производственных приложений

Направления работы ЦПБ

- Защита АСУ ТП и технологических приложений
- Консалтинг и аудит. Категорирование.
- Проектирование СОИБ
- Внедрение решений СОИБ
- Противодействие БПЛА.
- Защита БАС, PSIM
- Защита pLTE, ПОИБ
- Социотех
- Аналитика, предикатив, реагирование

Ключевые вопросы проектов Антидрон и защита БАС

31 января 2024 г., Президент России подписал закон, разрешающий сотрудникам служб транспортной безопасности сбивать беспилотные аппараты.
ФЗ о внесении изменений в отдельные законодательные акты РФ.

Противодействие боевым ударным БПЛА является задачей ПРО, ПВО и РЭБ страны.

Противодействие гражданским БВС, несущим угрозы промышленным предприятиям, как средство разведки, террора, хищений, - организуется ответственными руководителями предприятий как проект снижения рисков бизнеса.

- **Вопросы, которые надо решить, чтобы установить стационарную Антидрон систему на производственном предприятии РФ:**

- Ответственные организационно-штатные структуры
- Разрешительная документация
- Радиооборудование и программно-технические решения
- Строительные и мачтовые конструкции
- Порядок эксплуатации, порядок применения средств обнаружения и подавления
- Сервисная поддержка

Что нужно:

- Деньги
- Люди
- Смысл

Как надо:

- Защитить ценное
- Экономически эффективно
- Встроится в государственную и отраслевую систему

Мероприятия обнаружения, оповещения, защиты и инженерно-технической укрепленности

Защищенность бизнес приложений (ERP+) и производственных приложений (PLM+)

Перечни существующих типовых отраслевых объектов КИИ в различных сферах:
Связь: https://www.rans.ru/images/metrecKII.pdf
ТЭК: https://minenergo.gov.ru/opendata/7715847529-perechen-obektov-kii-2023
Химия; Горнодобывающая; Металлургия; ОПК: https://minpromtorg.gov.ru/activities/vgpp/vgpp4/perechni-tipovyh-obektov-kii
Транспорт: https://mintrans.gov.ru/documents/7/12506
Здравоохранение: https://portal.egisz.rosminzdrav.ru/materials/4525
Минтранс https://mintrans.gov.ru/documents/7/12506

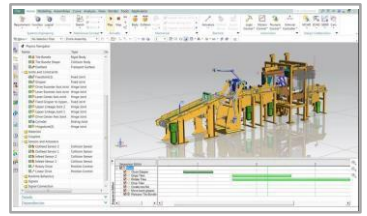
Перечень типовых объектов КИИ

15.	Система управления предприятием (ERP)	Учёт производства основной металлосодержащей продукции; Учёт вспомогательного производства; Регистрация выполнения производственной программы; Анализ исполнения производственной программы.
5	Система цифрового (автоматизированного) проектирования (CAD)	– Автоматизированное проектирование и подготовка производства изделий; – Автоматизированное проектирование конструкторской и технологической документации; – Автоматизированное проектирование механических или электронных устройств; – Автоматизированный выбор способа реализации процесса обработки (расчет разных способов реализации отдельных процессов.
6	Система управления жизненным циклом изделия (PLM)	– Управление информацией об изделиях на протяжении всех этапов их жизненного цикла.

Категория (AutoCAD) угроз блокируется на компьютерах технологических сетей, в том числе в сетевых папках и на рабочих станциях инженеров.

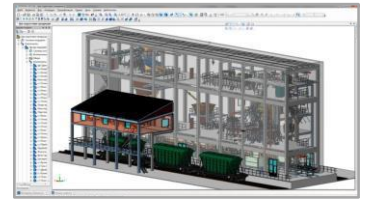
Решаемые задачи по мероприятиям защиты для следующих направлений:

1. Конструкторская подготовка производства, включая проектирование (трёхмерное моделирование) изделий и их составные части.
2. Технологическая подготовка производства.
3. Разработка конструкторской и технологической документации.
4. Управление инженерными данными и жизненным циклом изделий.



Модели технологических систем

PLM Software SIEMENS NX
DASSAULT SYSTEMES



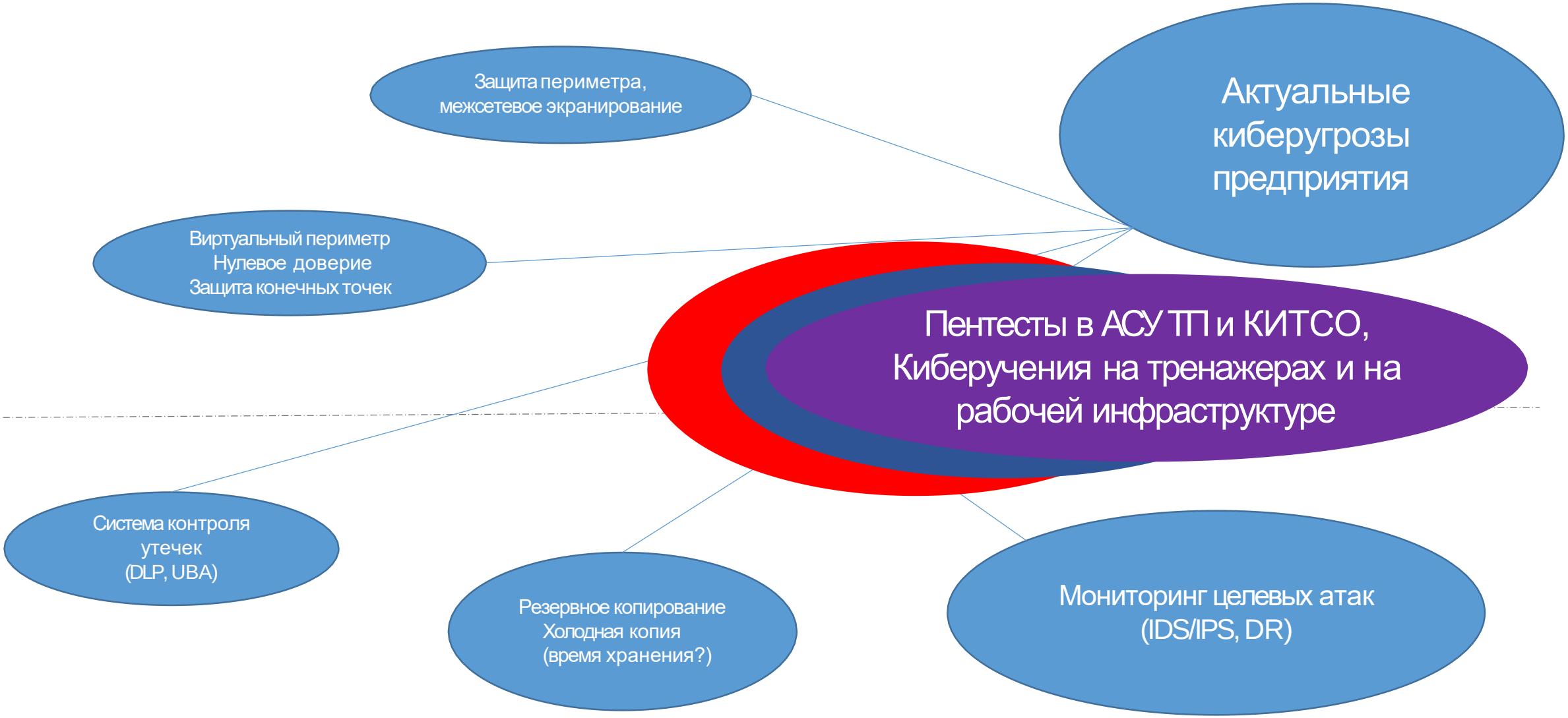
BIM-модели

Цифровые двойники изделий

Цифровое производство

Инженерно-технический документооборот

Организация противодействия киберугрозам



Актуальные киберугрозы для предприятий 2023-2024

Компрометация учетных записей, проникновения, другое

Остановка производственных процессов

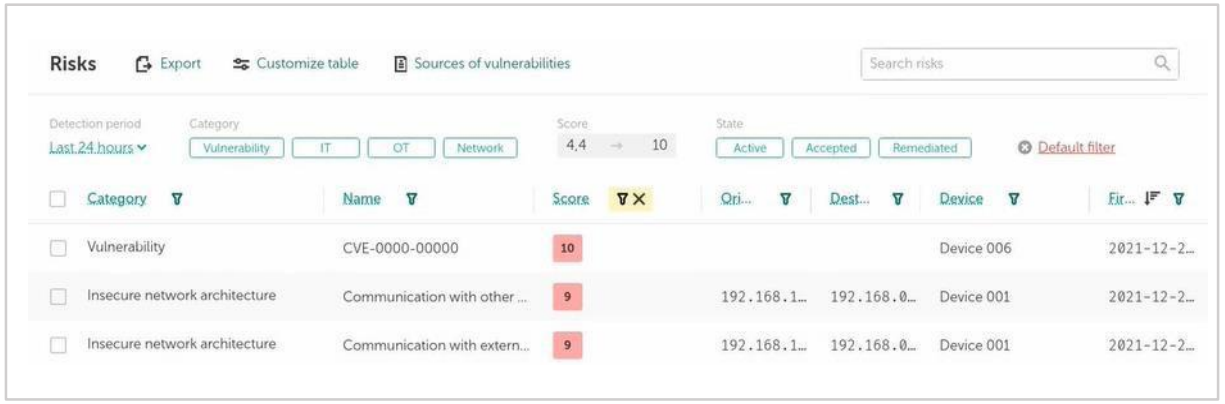
преступная халатность или вражеская активность

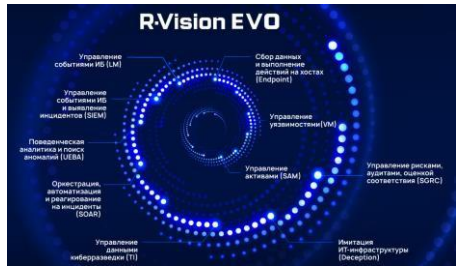
Деструктивная деятельность с непредсказуемыми последствиями

Ассоциация «Лига содействия оборонным предприятиям»

Средства защиты АСУ ТП

- Применяем инновации развития экосистем ЛК KICS и PT ICS





КОД БЕЗОПАСНОСТИ

- Проводим работы по развертыванию системы раннего обнаружения аномалий Kaspersky MLAD при проведении модернизации технологических объектов с заменой ПЛК и SCADA.

- Тестируем решения Kaspersky Secure Remote Workspace (KSRW) и Kaspersky IoT Secure Gateway (KISG)

UserGate

РусБИТех-Астра

- Разворачиваем новые СЗИ на российском Линуксе и российской виртуализации

Новые реалии в методологии и технологиях

- В связи с уходом зарубежных вендоров на предприятия идет выбор новых производителей технологических линий, ПЛК, SCADA систем (Россия, Китай, +). По аналогии с предыдущими западными вендорами возникает необходимость тестирования на совместимость с СЗИ, разбора методик харденинга, получение знаний о возможностях администрирования устройств и систем ААА.
- Особенно много вопросов возникает в связи со строительством новых объектов капитального строительства, закупки оборудования и новых РД РФ. В частности постановления Постановление Правительства РФ от 26 октября 2022 г. N 1912.

- Переход на российские операционные системы и прикладные продукты, виртуализация, замена почты, аппаратных и программных комплексов защиты (антивирусы, межсетевые экраны, системы удаленного доступа). Новые бренды серверов и сетевого оборудования.

- Глубоко прорабатывается замена технологий, обеспечивающих основное производство. Программных - ERP, MES, SCADA и технических - ПЛК и полевые компоненты.

- АРМы АСУ ТП по-прежнему остаются проблемой.

- Рост взаимосвязей систем СЗИ и реальная обработка больших массивов данных сетей АСУ ТП заставили системных интеграторов и производителей больше внимания уделять производительности.

Информзащита
Системный интегратор

Информационная безопасность 24x7x365

Центр противодействия кибератакам IZ SOC

+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru

Системный интегратор

+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Центр противодействия мошенничеству

antifraud@infosec.ru

Пресс-служба

pr@infosec.ru

Сервисный центр

+7 495 981 92 22
support@itsoc.ru
www.itsoc.ru