УЦСБ SOC

Промышленный SOC

Инструкция по применению

WHOAREWE

Модератор

ВАДИМ БОЧКАРЕВ

Коммерческий руководитель
УЦСБ SOC

Спикер

КОНСТАНТИН МУШОВЕЦ

Директор
УЦСБ SOC

Спикер

МАРИНА ЖУКОВА

Сервисный менеджер
УЦСБ SOC

О ЧЕМ ПОГОВОРИМ

01 Зачем нужен мониторинг в ОТ?

02 Недопустимые события в АСУ ТП

03 Примеры атак

04 Прагматичный мониторинг

УЦСБ SOC

ЗАЧЕМ НУЖЕН МОНИТОРИНГ ОТ-ИНФРАСТРУКТУРЫ

01

СОБЛЮДАТЬ ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА

02

НЕ ДОПУСТИТЬ РЕПУТАЦИОННЫЙ УЩЕРБ

!03

ПРЕДОТВРАТИТЬ ФИНАНСОВЫЕ ПОТЕРИ

ИСХОДНЫЕ ДАННЫЕ

- Зоопарк решений
- Недопустимость перезагрузки
- Критичность внесения изменений
- Соприкосновение интересов подразделений ИТ, ИБ и АСУ ТП
- Специализированные технологические протоколы
- Присутствие OT-вендоров с привилегированным доступом

ОГРАНИЧЕНИЯ ДЛЯ МОНИТОРИНГА

- Множественные уязвимости
- Невозможность применять оперативные меры реагирования
- Неприменимость инструментария для ИТ-инфраструктур

ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА ФЗ №187, ФЗ №58

01 Уведомление о компьютерных инцидентах

02 Планирование мероприятий по защите информации

03 Мониторинг и анализ рисков

04 Контроль и реагирование на инциденты

05 Использование современных технологий защиты

КАКИЕ ТРЕБОВАНИЯ МОЖНО РЕАЛИЗОВАТЬ С ПОМОЩЬЮ SOC

Условное обозначение	Меры защиты информации	Кол-во требований по классам защиты			
		К3	К2	К1	Всего
РСБ	Регистрация событий безопасности	7	8	8	9
СОВ	Обнаружение вторжений	0	0	3	3
ИПО	Информирование и обучение персонала	3	4	4	4
ИНЦ	Выявление инцидентов и реагирование на них	7	7	7	7

ПОДРОБНЕЕ О ТРЕБОВАНИЯХ ИНЦ И ИПО

РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ (ИНЦ)

- ИНЦ.0 Регламентация правил и процедур реагирования на компьютерные инциденты
- ИНЦ.1 Выявление компьютерных инцидентов
- ИНЦ.2 Информирование о компьютерных инцидентах
- ИНЦ.3 Анализ компьютерных инцидентов
- ИНЦ.4 Устранение последствий компьютерных инцидентов
- ИНЦ.5 Принятие мер по предотвращению повторного возникновения компьютерных инцидентов
- ИНЦ.6 Хранение и защита информации о компьютерных инцидентах

ИНФОРМИРОВАНИЕ И ОБУЧЕНИЕ ПЕРСОНАЛА (ИПО)

- ИПО.0 Регламентация правил и процедур информирования и обучения персонала
- ИПО.1 Информирование персонала об угрозах безопасности информации и о правилах безопасной работы
- ИПО.2 Обучение персонала правилам безопасной работы
- ИПО.3 Проведение практических занятий с персоналом по правилам безопасной работы
- ИПО.4 Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы

ВСТУПЛЕНИЕ В СИЛУ ТРЕБОВАНИЙ ФЗ №58

Изменения вступили в силу 1 сентября 2025 года

Субъектам КИИ рекомендуется:

01

Провести инвентаризацию существующих объектов ОКИИ, пересмотрев и рассчитав бюджет на замену иностранного оборудования в соответствии с будущими требованиями Правительства

02

Организовать взаимодействие с ГосСОПКА самостоятельно или через центры, имеющие соглашение с НКЦКИ – центры мониторинга и реагирования на инциденты

НЕДОПУСТИМЫЕ СОБЫТИЯ В ОТ

НС ДЛЯ АСУ ТП

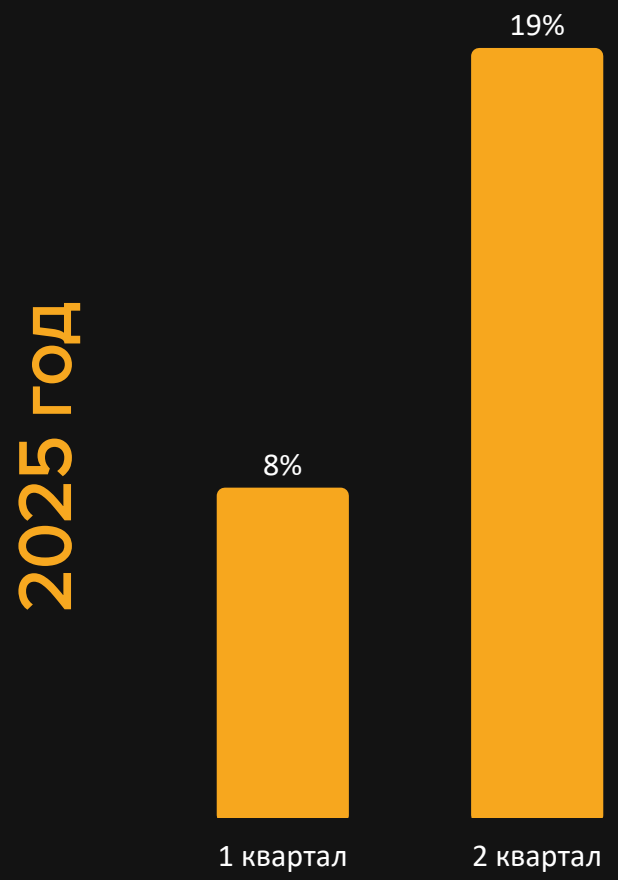
Недопустимое событие — событие, возникшее в результате кибератаки, которое делает невозможным достижение операционных и (или) стратегических целей организации или приводит к значительному нарушению ее основной деятельности

Для отрасли электроэнергетики	• системная авария — нарушение нормального режима работы энергетической системы; • отключение объектов электросетевого хозяйства, генерирующего оборудования; • нарушения в работе противоаварийной или режимной автоматики, влекущие за собой отключение объекта или прекращение электроснабжения; • нарушение логистических цепочек.
Для промышленных компаний	• нарушение технологического процесса и прерывание функционирования, • компрометация конфиденциальной информации, • возможность вывода денежных средств со счетов компании, • искажение или утрата рабочих данных и функциональных сведений, • использование вычислительных мощностей для атак на другие компании.
Для промышленных предприятий, которые применяют технологию интернета вещей	• остановка технологического процесса на основе IIoT является самой значимой угрозой информационной безопасности промышленного интернета вещей • простои в работе платформенного IIoT-решения и нарушение целостности информации, циркулирующей в IIoT-инфраструктуре, ее искажение • потеря контроля управления технологическим процессом на основе IIoT • потеря и утечка чувствительной информации и использование IIoT-инфраструктуры как промежуточного сегмента для атаки на внутреннюю ИТ-инфраструктуру

ПРИМЕРЫ

КИБЕРАТАК НА ОТ

ПРОМЫШЛЕННОСТЬ ТОЖЕ АТАКУЮТ



Одна из причин — высокая вероятность получения выкупа

Предприятия настолько заинтересованы в бесперебойной работе и непрерывности производственных процессов, что готовы платить любой «гонорар»

ПРИМЕРЫ АТАК

Кейс №1

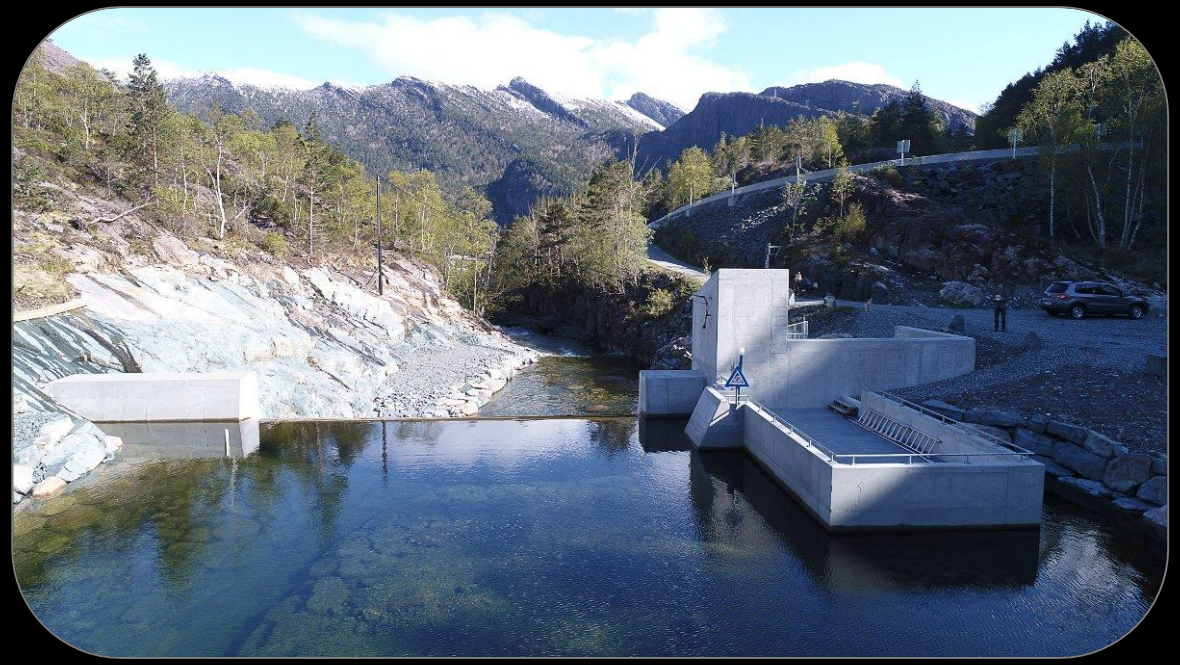
Апрель 2025

Взлом системы управления плотиной в норвежской коммуне Бремангер.

Результат: открыт клапан сброса воды.
Потеря контроля над сбросом воды в течении 4 часов.

Расследование: использование слабого пароля для доступа к web-интерфейсу управления клапаном.

Выявленные слабые места: применение web-интерфейса для управления критической частью процесса. Отсутствие аудита для отслеживания множественных попыток подбора пароля



ПРИМЕРЫ АТАК

Кейс №2

Сентябрь 2025

Остановка работы аэропортов Брюсселя, Хитроу в Лондоне, Бранденбург в Берлине

Результат: полностью отключена система регистрации на 10 часов, что повлекло огромные финансовые убытки

Расследование: взломан поставщик системы регистрации на рейс, которая использовалась в упомянутых аэропортах, и предоставлялась компанией Collins Aerospace.

Выявленные слабые места: атака на цепочку поставок

ПРИМЕРЫ АТАК

Кейс №3

Август-сентябрь 2025

Кибератака на автопроизводителя Jaguar Land Rover (JLR)

Результат: практически полная остановка завода по сборке. Поломка цепочки поставок.

Расследование: официальной информации еще нет, расследование продолжается. Предположительно, шифровальщик, источник попадания ВПО неизвестен.

Последствия: самые масштабные за всю историю британского бизнеса: 3 000 сотрудников отправлены в отпуск, полное восстановление не ранее 2026 года, правительство выдало гос. кредит на восстановление.

ПРИМЕРЫ АТАК

Кейс №4

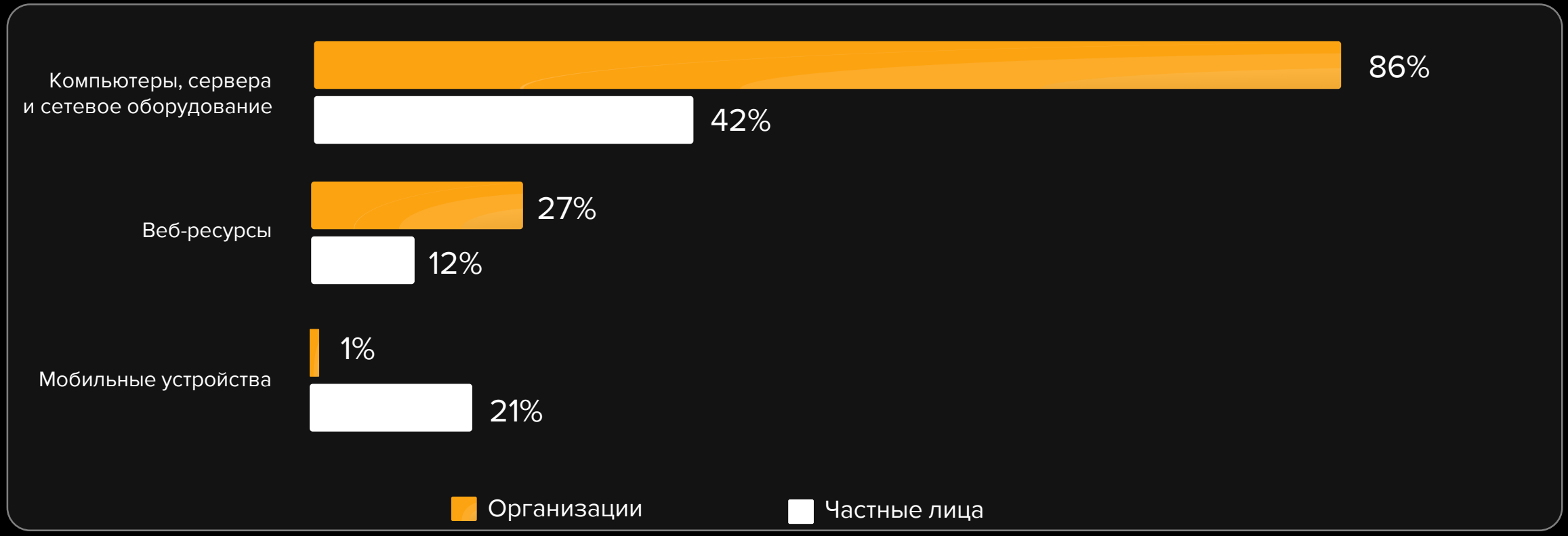
Сентябрь 2025

Взлом электронных бегущих строк в аптеках и магазинах, чтобы выводить мемы, матерные выражения и экстремистскую символику

Результат: репутационный ущерб и возможная и статья за экстремистское содержание текста

Расследование: скачали приложение управления панелью, подключились к открытой сети Wi-Fi и ввели заводской пароль, который владельцы не меняли

ЧТО НА ПРОИЗВОДСТВАХ АТАКУЮТ ЧАЩЕ



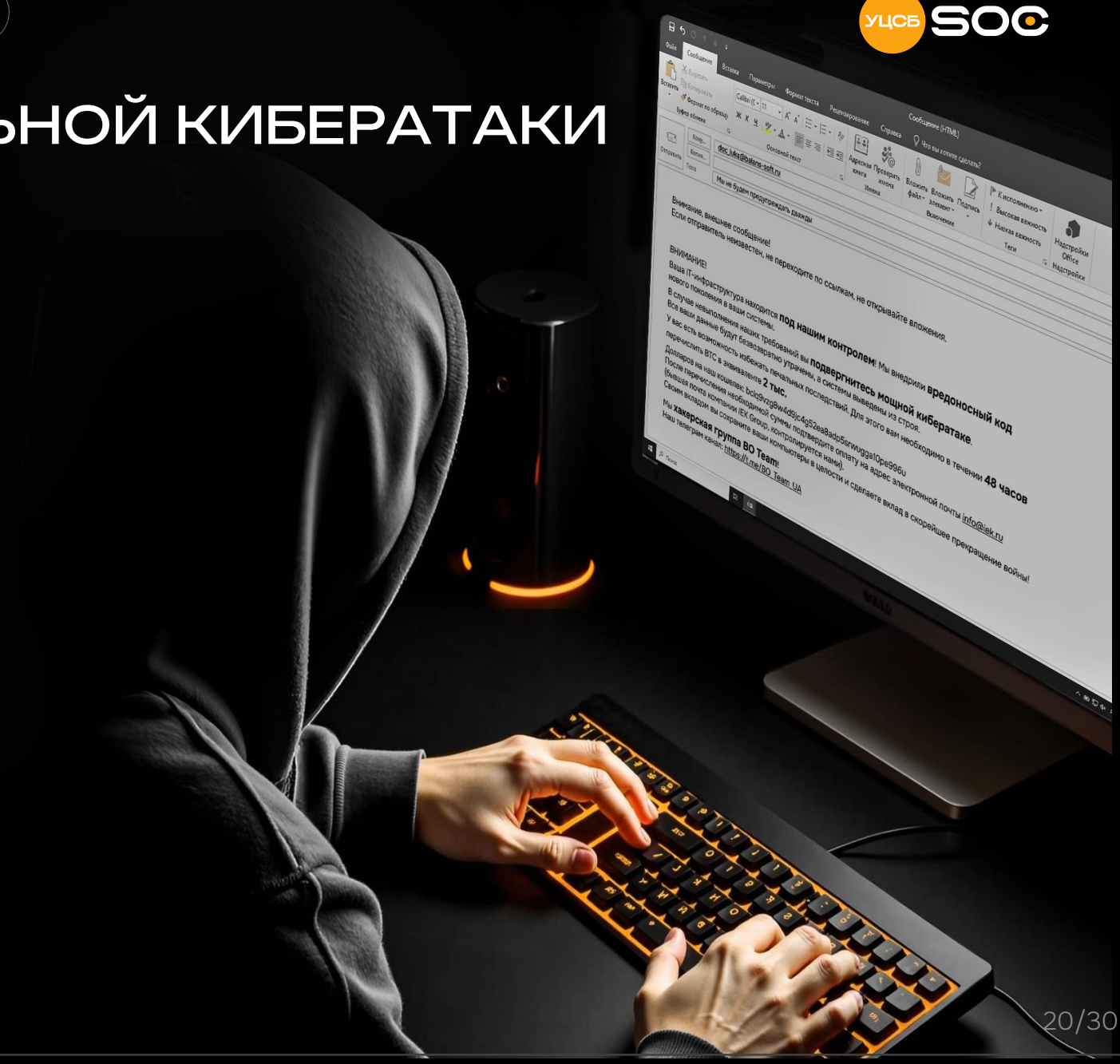
Новая тактика: требуют выкуп не за зашифрованные данные, а за нераскрытие уязвимостей программного обеспечения

Статистика PT за 1 квартал 2025 года

РАЗБОР ВЕКТОРА РЕАЛЬНОЙ КИБЕРАТАКИ

Сервер и backup зашифрованы.

Чтобы получить ключ дешифровки переведите в криптовалюте.



РАЗБОР ВЕКТОРА РЕАЛЬНОЙ КИБЕРАТАКИ

Атака

Получение физического доступа и авторизация под УЗ администратора ПК-SCADA

↓

Отключение антивируса и агента SIEM

↓

С помощью SCADA изменение скрипта PLC

↓

Завершение работы SCADA, запуск шифровальщика с USB-носителя

↓

Шифрование backup

→

Недочеты мониторинга

1. Отсутствие контроля подключения USB-носителей
2. Отсутствие контроля изменения конфигурации СЗИ
3. Отсутствие контроля внесения изменений в PLC

УЦСБ SOC

ПРАГМАТИЧНЫЙ МОНИТОРИНГ

ПОДГОТОВКА

00 Сформировать задачи мониторинга ИБ: недопустимые события, модель угроз и др.

01 Обеспечить регулярную инструментальную инвентаризацию сети

02 Реализовать управление активами (не бумажное!)

03 Реализовать регулярную инвентаризацию периметра OT-инфраструктуры

04 Обеспечить максимальное покрытие сети САВЗ

05 Обеспечить журналирование необходимых событий безопасности

06 Обеспечить выделенные рабочие станции для OT-вендоров и подрядчиков

ПРИНЦИПЫ МОНИТОРИНГА

- Реализуем безагентский мониторинг без функций активного реагирования
- Применяем анализ трафика на предмет выявления аномальной активности
- Отслеживаем время активности администраторов и пользователей
- Отслеживаем действия на среднем уровне: передача админ.команд, воздействие через API и т.п.
- Обеспечиваем контроль работы с внешними носителями
- Контроль подключения хостов к сети
- Контроль выделенных рабочих станций ОТ-вендоров и подрядчиков
- Перечень учетных записей привилегированных пользователей
- Compliance и контроль изменения конфигурации критичных узлов
- Не забываем про контроль доступности источников событий

ПЕРЕЧЕНЬ ИСТОЧНИКОВ СОБЫТИЙ

01 АРМ операторов

02 АРМ администраторов и программистов PLC

03 Выделенные АРМ для ОТ-вендоров и подрядчиков

04 Серверное оборудование

05 Активное сетевое оборудование

06 Средства защиты информации

07 Контроллеры домена/AAA

08 Специализированное ПО

09 Устройства среднего уровня

10 Периметр ОТ-инфраструктуры

УЦСБ SOC — ЦЕНТР МОНИТОРИНГА КИБЕРБЕЗОПАСНОСТИ

Мы сопровождаем весь процесс: от выявления инцидента до его полной нейтрализации, устранения последствий и принятия мер по предотвращению его повторного возникновения.

БЫСТРЫЙ СТАРТ

Настроим мониторинг в течение 14 дней

ГИБКИЙ ПОДХОД

Подстроим сервис под ваши потребности

ШИРОКАЯ ЭКСПЕРТИЗА

Привлекаем экспертов УЦСБ из различных сегментов ИБ

24/7

режим оказания услуг

> 5 лет

на рынке информационной безопасности

< 15 минут

реакция на инцидент ИБ

98%

продленных контрактов

О КОМПАНИИ УЦСБ

с 2007
экспертиза в ИТ и ИБ

> 900
профессионалов в штате

> 4000
завершенных проектов

Входим в список 100 крупнейших компаний России в сфере защиты информации и ИТ по версии CNews Analytics и TAdviser

КОМПЕТЕНЦИИ

- Информационная безопасность
- Информационные технологии
- Анализ защищенности
- Центры обработки данных
- Инженерно-технические средства охраны
- Интеллектуальные инженерные системы
- Сервисный центр

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ

УЦСБ SOC

ВОПРОСЫ?

УЦСБ SOC

Security Operations Center

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ

soc@ussc.ru

soc.ussc.ru