



ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

7 ПРОБЛЕМ

ПРИ СОЗДАНИИ СОИБ АСУ ТП
В 2025 ГОДУ



Докладчик

Алексей Комаров

Региональный представитель



Автор презентации

Анна Почечуева

Пресейл-инженер

Уральский центр систем безопасности (УЦСБ)

> 17

лет на рынке

> 1000

профессионалов в штате

> 4000

реализованных проектов

Топ-100 крупнейших отечественных ИТ-компаний ¹

Топ-15 крупнейших компаний России в сфере защиты информации ²

Компетенции

- Информационная безопасность
- Информационные технологии

¹Рейтинг CNews100: Крупнейшие ИТ-компании России 2023

²Рейтинг CNews Security: Крупнейшие компании России в сфере защиты информации 2023

ПРОБЛЕМЫ

Морально
устаревшие
продукты

Неготовность
инфраструктуры

Ограниченный
функционал
отечественных
решений

Человеческий
фактор

Безопасная
разработка

Обновление ИТ
и ИБ решений

Требования законодательства.
Отраслевая специфика

7

ПРОБЛЕМ



01 | Невозможность использования морально устаревших продуктов

Проблема

- ППО для АСУ ТП способно функционировать только на ОС Windows
- Модернизация не учитывает импортозамещение
- Техническая и сервисная поддержка более недоступна
- Для средств защиты рекомендованы к использованию иностранные программные средства

01 | Невозможность использования морально устаревших продуктов

Результат



«... с 1 января 2025 г. ... запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, ... либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, ... а также пользоваться сервисами (работами, услугами) по обеспечению информационной безопасности, предоставляемыми (выполняемыми, оказываемыми)» этими организациями.

Указ Президента РФ от 1 мая 2022 г. N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

Решение



- Использование наложенных средств защиты, средств мониторинга
- Усиление организационных и компенсирующих мероприятий, использование мер промышленной, физической и иной безопасности
- Внесение корректирующих мероприятий в рамках модернизаций

02 | Неготовность инфраструктуры

Проблема

- АСУ ТП создавалась на основе актуальных требований
- Разнородная инфраструктура, «зоопарк» программно-аппаратного обеспечения

02 | Неготовность инфраструктуры

Результат



- Отсутствует упорядоченность, прозрачность IT-активов
- Затруднена интеграция вновь проектируемых технологических решений и средств безопасности
- Инженерная инфраструктура не способна к обеспечению новых систем

Решение



- Упорядочение инфраструктуры «вне очереди», формирование дорожной карты
- Масштабирование в рамках модернизаций

03 | Ограниченный функционал отечественных решений

Проблема

- Маркетинговые заявления не соответствуют действительности
- Функционал недостаточен на фоне импортных решений

03 | Ограниченный функционал отечественных решений

Результат



- Затруднена интеграция вновь проектируемых технологических решений и средств безопасности
- Невозможно сохранение функционала ранее спроектированных СОИБ в полной мере
- Вынужденное использование дополнительных мер безопасности

Решение



- Формирование и поддержание уровня компетенций на основании сильной экспертизы
- Лаборатории и предварительное пилотирование продуктов

04 | Требования законодательства. Отраслевая специфика

Проблема

- Отсутствие единой трактовки законодательных требований
- Планы перехода на отечественное оборудование часто не включают ландшафт ИБ
- Потребность в перекатегорировании
- Доверенные ПАКи

04 | Требования законодательства. Отраслевая специфика

Результат



Изменения вносятся в проект чаще, чем это возможно совершить бесшовно, что неизбежно приводит к конфликту исходных задач и фактического результата

Решение



- Самостоятельное поддержание состояния результатов категорирования с использованием средств автоматизации
- Привлечение организаций с широким опытом и экспертизой

05 | Обновление ИТ и ИБ решений

Проблема

- Изменение продуктовых линеек
- Обновление политик лицензирования
- EOS|EOL продуктов, отказ от продления сертификатов соответствия

05 | Обновление ИТ и ИБ решений

Результат



Требуется в краткие сроки в рамках проектного цикла применить изменения, как «на бумаге», так и «в полях»

Решение



- При формировании требований к Исполнителю требуется уделить внимание опыту, объему компетенций, имидж среди партнеров (импортных, отечественных)
- Привлечение организаций с широким опытом и экспертизой

06 | Безопасная разработка

Проблема

- Безопасная разработка начинается с модернизации

«... 29.3 Прикладное программное обеспечение, планируемое к внедрению в рамках создания (модернизации или реконструкции, ремонта) значимого объекта и обеспечивающее выполнение его функций по назначению (далее – программное обеспечение), должно соответствовать следующим требованиям по безопасности:...»

Приказ от 25 декабря 2017 г. N 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

- Эшелонированная защита
- Отсутствие единой трактовки законодательных требований
- Низкий уровень защищенности ППО АСУ ТП

06 | Безопасная разработка

Результат



- Рост объема работ в отрыве от реального повышения уровня защищенности
- Увеличение поверхности атак

Решение



- Самостоятельное обеспечение должного уровня безопасной разработки, сторонний консалтинг
- Использование технических средств, обогащенных экспертизой, использование облачных средств для непрерывного анализа



07 | Человеческий фактор

Проблема

- Отсутствие границ зон ответственности (АСУ ТП, ИБ, ИТ) и внутренних коммуникаций
- Недостаточный уровень компетенций

07 | Человеческий фактор







ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

**СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?**

Алексей Комаров

Региональный представитель

sec.USSC.RU



cybersec@ussc.ru

