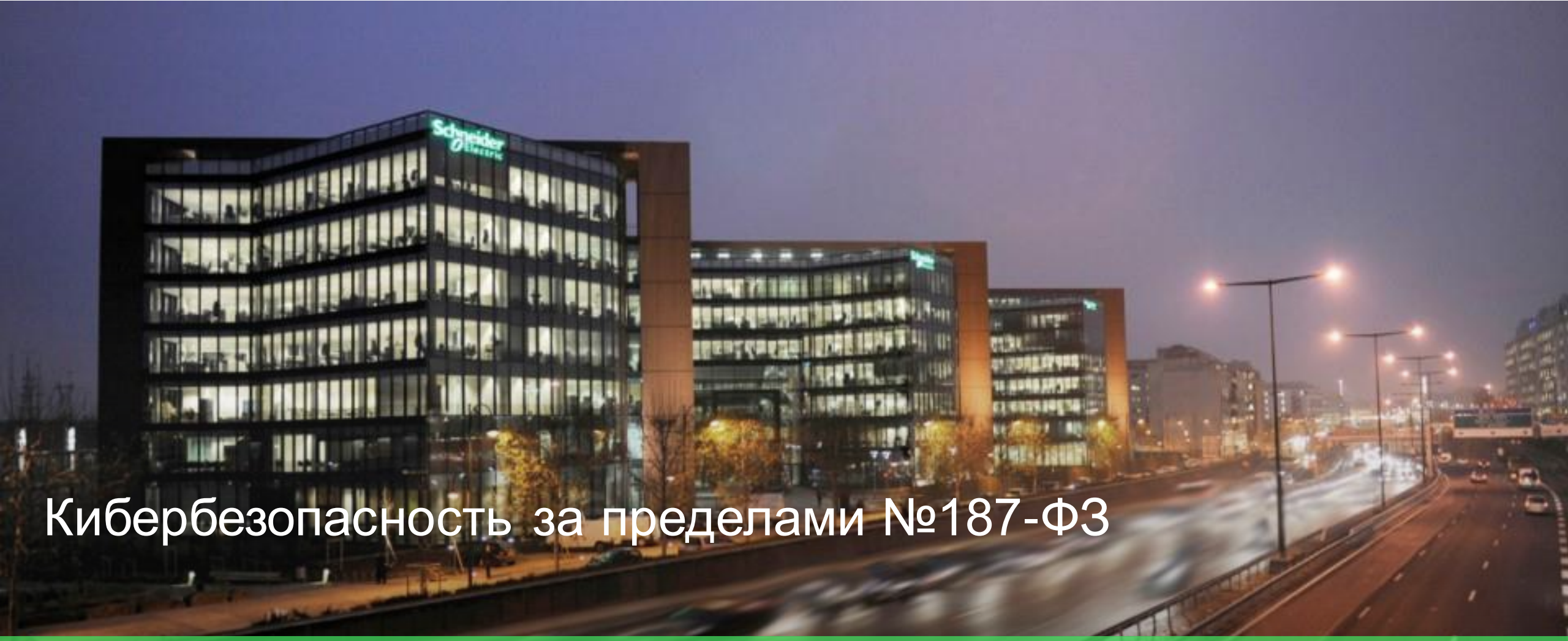


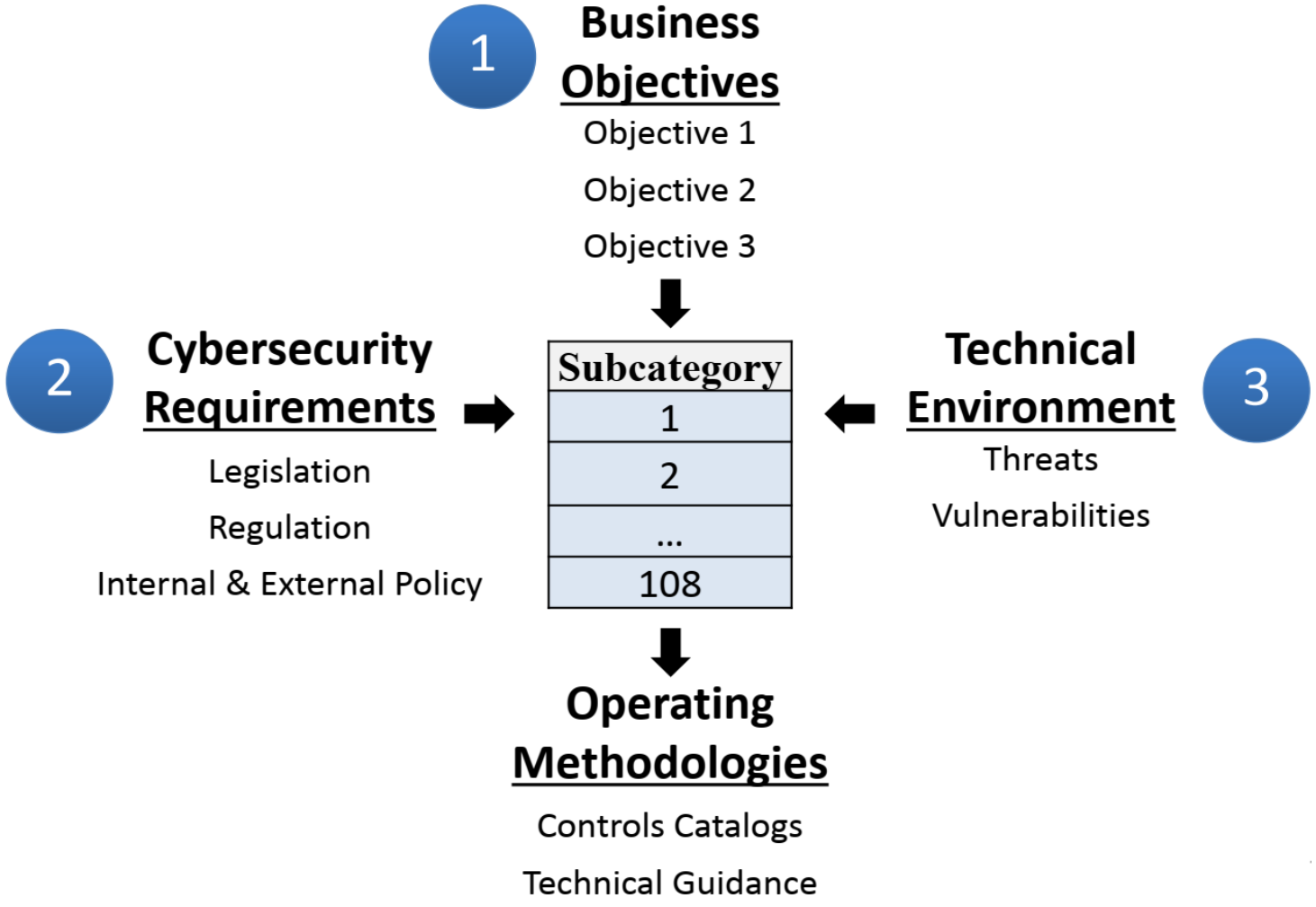
Кибербезопасность за пределами №187-ФЗ

Ян Андреевич Сухих
Руководитель направления ИБ
АО «Шнейдер Электрик»

Подходы к информационной безопасности (РФ vs США)

Подходы к защите КИИ (Россия vs США)

Подход в США



Подход в России

Подходы к защите КИИ (Россия vs США)

CISA (under DHS)

Cybersecurity and Infrastructure Security Agency (CISA) under Department of Homeland Security (DHS)

National Cybersecurity and Communications Integration Center (NCCIC)	Critical Infrastructure Cyber Community Voluntary Program (C^3VP)	National Infrastructure Coordinating Center
С 2009 года выступает как интеграционный хаб для информации связанной с ИБ, как центр технических компетенций, аналитики и центр по реагированию на инциденты	Добровольная программа/партнерство DHS с собственниками КИ с целью продвижения и популяризации риск-ориентированного подхода, NIST framework for improving critical infrastructure cybersecurity	Координация активностей, обмен информацией между государственными структурами и субъектами КИ при возникновении инцидента с целью минимизации последствий.
Аналог в РФ – НКЦКИ (ГосСОПКА), ФСБ	Аналогов нет/187-ФЗ + УК 274.1	Аналогов нет, создается комиссия

Методология для построения комплексных систем кибербезопасности. Framework for Improving Critical Infrastructure Cybersecurity, NIST

Структура фреймворка

Функции

- Identify/Идентификация
- Protect/Защита
- Detect/Обнаружение
- Respond/Реагирование
- Recover/Восстановление

- Функции позволяют структурировать активности по основным направления деятельности в области кибербезопасности
- Каждая функция делится на категории и подкатегории, которые детально раскрывают их суть
- Подкатегории ориентированы не на продукты/решения, но на меры, которые должны быть реализованы в организации

Пример риск-ориентированного подхода

Безопасность в промышленности

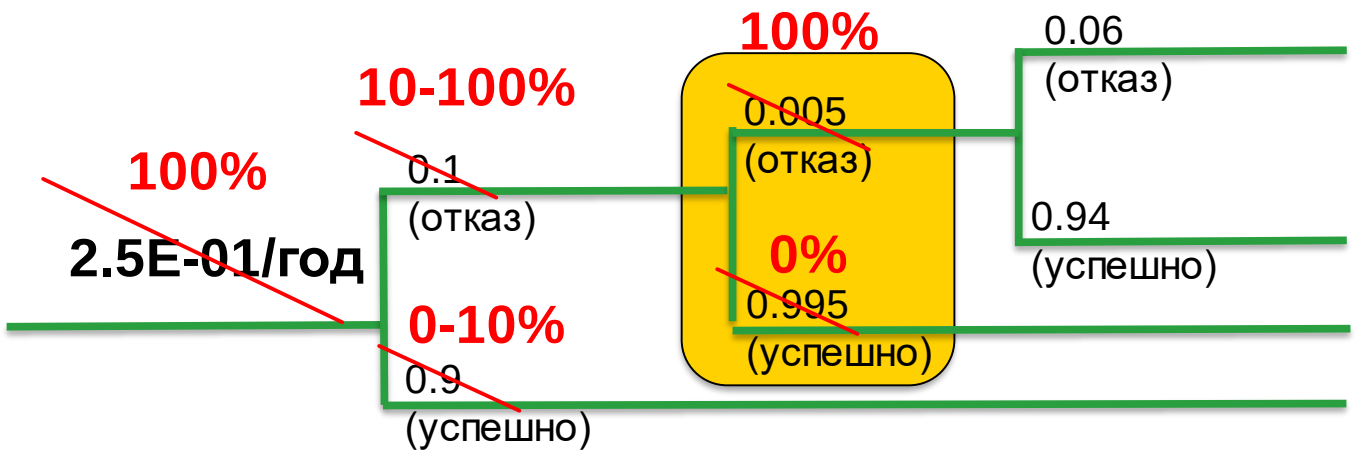
Модель слоев защит / Модель «швейцарского сыра» (Swiss cheese model)

Как происходят аварии и возможная роль кибератак в ней

Возможные последствия кибератаки

Диаграмма LOPA (дерево отказов) до и после успешной кибератаки

Событие	СЛОЙ ЗАЩИТЫ №1	СЛОЙ ЗАЩИТЫ №2	СЛОЙ ЗАЩИТЫ №3	Результат	Частота
Отказ контура регулирования давления	Действия оператора на сигнализацию	SIL 2 → SIF	Предохранительный клапан		



Допустимая частота = 1.0E-05

…а нет ли подхода попроще?

1. Какие активы находятся в зоне риска? Расставлены ли приоритеты и определены ли последствия если АСУ ТП будут скомпрометированы? Сможем ли мы продолжать работу на установке после успешной кибератаки? А что если..?
2. Кто ответственный за кибербезопасность? Назначены ли ответственные за ИБ в целом по предприятию и/или за данную конкретную установку/ИС
3. Подключены ли наши АСУ ТП к внешним сетям? Если нет, то как мы можем в этом убедиться?
4. Есть ли удаленный доступ к АСУ ТП? Если да, то насколько на самом деле он нам нужен/можно ли без него обойтись? Как обеспечена защита удаленного доступа, включая защиту инфраструктуры подрядчика
5. Используются ли лучшие практики? Осведомлены ли ваши сотрудники о лучших мировых практиках в области ИБ, используются ли они для защиты ваших активов?
6. Подключены ли вы к ГосСОПКА? Подключение к ГосСОПКА, при ее должном развитии, будет иметь огромное влияние на кибербезопасность отрасли в целом и вашей компании в частности.

Наше предложение для рынка ИБ АСУТП

Лицензии

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер 3582 от 29 марта 2019 г.

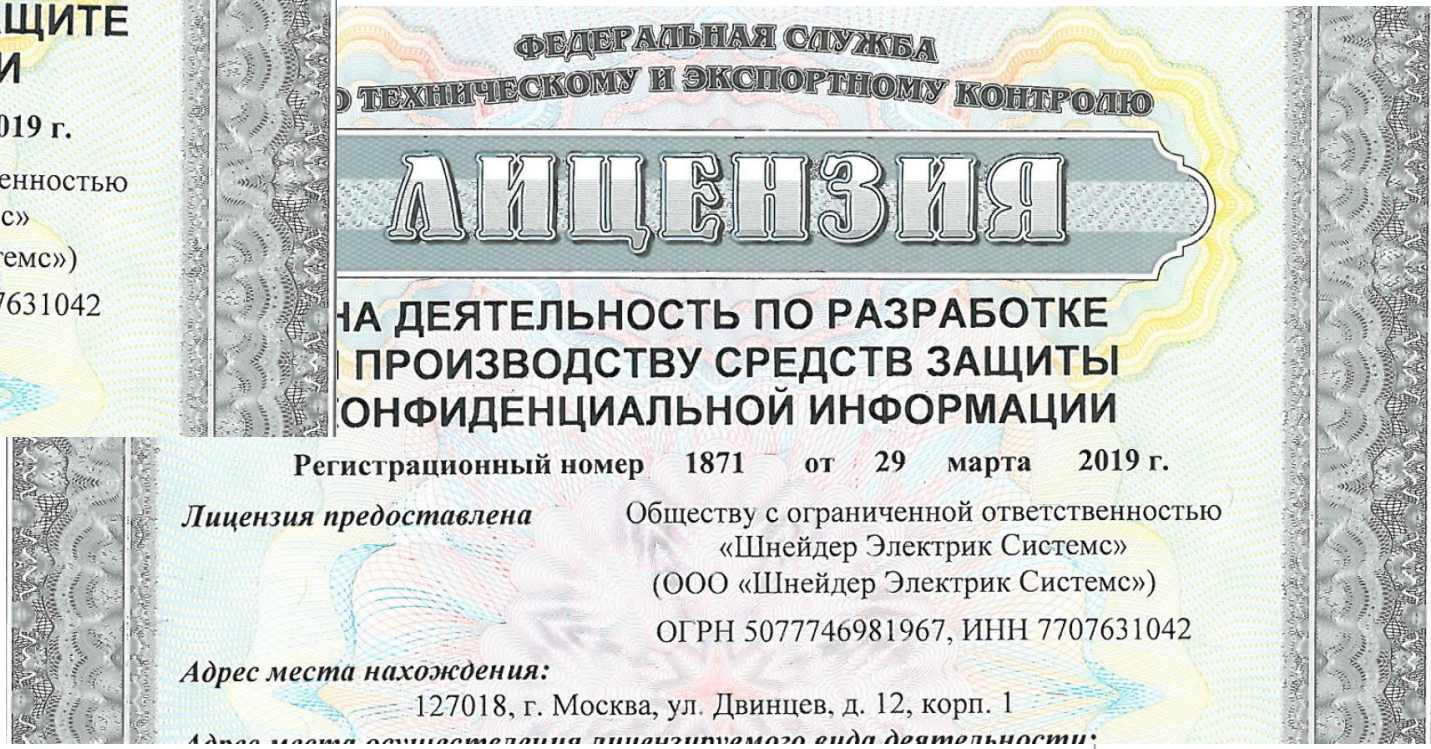
Лицензия предоставлена Обществу с ограниченной ответственностью «Шнейдер Электрик Системс» (ООО «Шнейдер Электрик Системс»)

ОГРН 5077746981967, ИНН 7707631042

Адрес места нахождения:

127018, г. Москва, ул. Двинцев, д. 12, корп. 1

Адрес места осуществления лицензируемого вида деятельности:



ФЕДЕРАЛЬНАЯ СЛУЖБА
О ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО РАЗРАБОТКЕ
ПРОИЗВОДСТВУ СРЕДСТВ ЗАЩИТЫ
ОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер 1871 от 29 марта 2019 г.

Лицензия предоставлена Обществу с ограниченной ответственностью «Шнейдер Электрик Системс» (ООО «Шнейдер Электрик Системс»)

ОГРН 5077746981967, ИНН 7707631042

Адрес места нахождения:

127018, г. Москва, ул. Двинцев, д. 12, корп. 1

Наше предложение

Консалтинг

От уровня АСУ ТП до SIEM и интеграции с ГосСОПКА:

Аудит

Комплексный аудит предприятий от полевого уровня до корпоративных систем на предмет защищенности

Тестирование комплексных решений

От уровня АСУ ТП до SIEM с использованием оборудования и ПО разных вендоров ИБ

Проектирование и внедрение

Защищенные АСУ ТП, DMZ, Интеграция IT и OT, внедрение IDS, IPS и т.п., интеграция с ГосСОПКА

Обслуживание и сервис

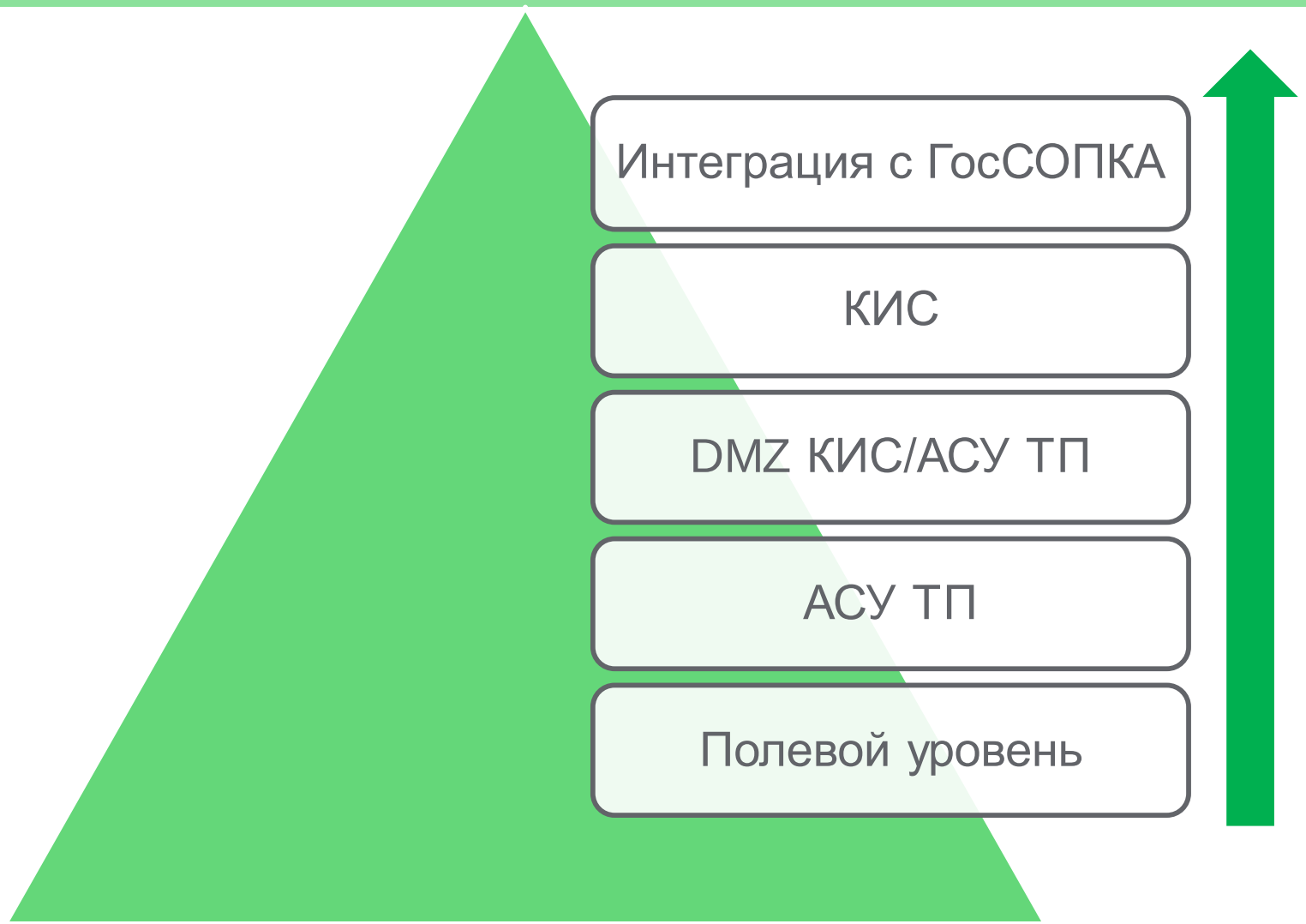
Ежегодные аудиты, тренинги

НИОКР/Исследования

Решение нестандартных задач, разработка уникального ПО

Категорирование

Предлагаем услуги и программное обеспечение для автоматизации процесса категорирования



НИОКР центр в Иннополисе

1. Развернут демо-стенд защищенной АСУ ТП. Включая ПЛК Modicon, РСУ Foxboro, ПАЗ Triconex, внедрены различные СрЗИ (АВЗ, СОВ, СПВ, МСЭ, AD, логирование, управление обновлениями и т.д), выполнен hardening ОС, организована DMZ
2. Реализована интеграция АСУ ТП с SOC наших партнеров. Можно в реальном времени посмотреть как работает SOC в случае имитации атаки на АСУ ТП
3. Интеграция с бизнес системами. В ближайшее время планируется интегрировать демо-стенд с решениями по реагированию на инциденты, управлению уязвимостями.

4. Проводятся пентесты защищенной АСУ ТП. С целью подтверждения надежность данной конкретной архитектуры и подхода к построению защищенных АСУ ТП в целом в R&D центре проводятся пентесты.


СПАСИБО!

Сухих Ян Андреевич

Руководитель направления ИБ

АО «Шнейдер Электрик»

M: +7 910 475 1750

D: +7 495 777 999 0 ext. 1268

E: yan.sukhikh@se.com