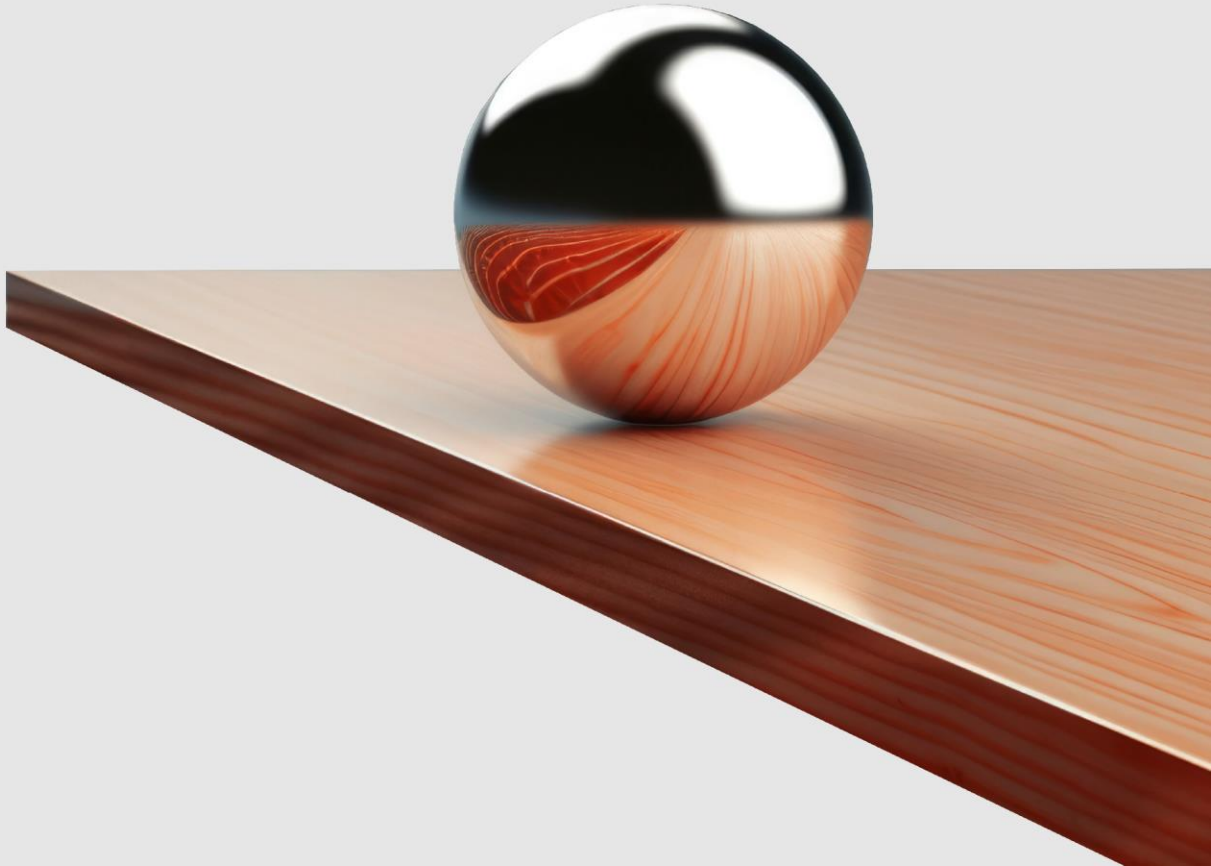
AKTIV.
CONSULTING

Защита ОКИИ на базе АСУ без влияния на конструктив

Ольга Копейкина

Ведущий консультант



Распространенные проблемы

После **проведения категорирования систем на базе АСУ** часто мы сталкиваемся со следующими нюансами:

Распространенные проблемы

После **проведения категорирования систем на базе АСУ** часто мы сталкиваемся со следующими нюансами:

Изначально система проектировалась без учета требований безопасности и не предполагает подключения средств защиты

Распространенные проблемы

После **проведения категорирования систем на базе АСУ** часто мы сталкиваемся со следующими нюансами:

Разработчики системы не заинтересованы перерабатывать конструктив в связи с требованиями безопасности или вообще уже не существуют

AKTIV.CONSULTING

Распространенные проблемы

После **проведения категорирования систем на базе АСУ** часто мы сталкиваемся со следующими нюансами:

Система проектировалась и создавалась давно, существенные модернизации не проводились, в следствии чего ПАК не предполагает построения на своей базе системы защиты

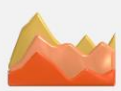
Распространенные проблемы

После **проведения категорирования систем на базе АСУ** часто мы сталкиваемся со следующими нюансами:

Систем большое количество,
и затраты на построение систем защиты информации на каждую неприемлемо высоки

Стандартный подход

Каждая система, задействованная в ключевом бизнес-процессе – **это объект КИИ,** на который распространяются требования по обеспечению безопасности.



Проектирование системы защиты

Разработка комплекта ОРД

Закупка оборудования и ПО

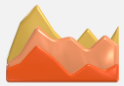
Периодическое продление лицензий и амортизация

Молитвы о том, чтобы система не перестала работать

Внедрение системы защиты

Стандартный подход

Проектирование системы защиты



Разработка комплекта ОРД

Периодическое продление лицензий и амортизация

Закупка оборудования и ПО

Молитвы о том, чтобы система не перестала работать

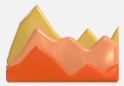
Внедрение системы защиты

Количество систем

AKTIV.CONSULTING

Стандартный подход

Проектирование системы защиты



Разработка комплекта ОРД

Периодическое продление лицензий и амортизация

Закупка оборудования и ПО

Молитвы о том, чтобы система не перестала работать

Внедрение системы защиты

×

Количество систем

=

Путь минимизации затрат

Сокращение затрат возможно за счет обобщения смежных систем в один объект КИИ.

Этот путь уместен, если:

системы территориально локализованы

системы взаимодействуют друг с другом в рамках одного БП

системы связывает одно недопустимое событие

Путь
минимизации затрат

Плюсом будет, если:

1

у систем одно или смежные эксплуатирующие подразделения

2

у систем один разработчик

Пример обобщения систем в один ОКИИ

*Приведенная схема не является реально существующей. Все данные для моделирования получены из общедоступных источников, не имеют пометок о конфиденциальности и представлены намерено обобщенно и приблизительно с целью исключительно приведения примера в образовательных целях.

Пример обобщения систем в один ОКИИ

Стандартный подход

Перед нами 8 объектов КИИ с (возможно) различной категорией значимости

Пример обобщения систем в один ОКИИ

Стандартный подход

Перед нами 8 объектов КИИ с (возможно) различной категорией значимости

Подход с обобщением

Анализ данных о представленных системах показывает следующие связи:

1. Технологический процесс – заправка ЖК
2. Бизнес процесс – пуск РН
3. Недопустимые события общие:
   - авария в ходе заправки
   - срыв пуска ракеты-носителя
4. Эксплуатирующее подразделение

Пример обобщения систем в один ОКИИ

Стандартный подход

Перед нами 8 объектов КИИ с (возможно) различной категорией значимости

Вывод

Перед нами
1 объект КИИ
~3 категорией значимости

Подход с обобщением

Анализ данных о представленных системах показывает следующие связи:

1. Технологический процесс – заправка ЖК
2. Бизнес процесс – пуск РН
3. Недопустимые события общие:
   - авария в ходе заправки
   - срыв пуска ракеты-носителя
4. Эксплуатирующее подразделение

Как это работает?

Что необходимо учитывать?

Сокращение финансирования на внедрение мероприятий по защите информации

Выполнение требований регуляторов **без влияния на рабочие процессы систем**

Управляемость и прозрачность действий администраторов и операторов комплекса систем

Формирование **единой точки ввода** и вывода информации в защищенном исполнении

Комплект ОРД и администратор безопасности **в единственном числе**

Что необходимо учитывать?

Выход из строя узла взаимодействия между системами **остановит бизнес-процесс полностью** до восстановления работоспособности

Большие сроки реализации с учетом необходимости привлечения разработчиков всех задействованных систем

Что необходимо учитывать?

ОКИИ будет иметь категорию значимости исходя **из наивысшей категории** входящих в него систем

В ОРД по-прежнему необходимо учесть **ВСЕ системы,** которые включаются в ОКИИ

Должны быть четкие основания **для обобщения объектов в один ОКИИ** для регуляторов

Что насчет импортозамещения?

Реализация представленной концепции позволяет пошагово выполнить импортозамещение и исполнение Указа Президента РФ от 1 мая 2022 г. N 250 на защищаемых объектах

1. Система обеспечения информационной безопасности может быть сразу выстроена на основе отечественных средств защиты

2. Внесение в состав защищаемых систем изменений в части импортозамещения не привязано к построению системы защиты и может проводиться в рамках плановых модернизаций по согласованию с регуляторами

3. Даже если в защищаемых системах есть отличия в конфигурации оборудования или ПО, это не влечет за собой существенных изменений в системе защиты и взаимодействия

Где искать кадры?

Специалист по ИБ	Знает все про вопросы информационной безопасности	Не знает ничего о промышленных системах, которые надо защищать
Инженер	Знает все о работе ключевых систем, используемых в организации и промышленной безопасности	Не знает ничего об информационной безопасности

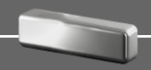
Где искать кадры?

Специалист по ИБ	Знает все про вопросы информационной безопасности	Не знает ничего о промышленных системах, которые надо защищать
Инженер	Знает все о работе ключевых систем, используемых в организации и промышленной безопасности	Не знает ничего об информационной безопасности
IT-специалист		

Где искать кадры?

Специалист по ИБ	Знает все про вопросы информационной безопасности	Не знает ничего о промышленных системах, которые надо защищать
Инженер	Знает все о работе ключевых систем, используемых в организации и промышленной безопасности	Не знает ничего об информационной безопасности
IT-специалист	Может помочь в части выстраивания инфраструктуры или настройки ПО	

Где искать кадры?



Специалист по ИБ	Знает все про вопросы информационной безопасности	Не знает ничего о промышленных системах, которые надо защищать
Инженер	Знает все о работе ключевых систем, используемых в организации и промышленной безопасности	Не знает ничего об информационной безопасности
IT-специалист	Может помочь в части выстраивания инфраструктуры или настройки ПО	Но он тут по большому счету ни при чем!

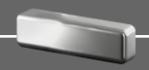
Где искать кадры?

Специалист по ИБ	Знает все про вопросы информационной безопасности	Не знает ничего о промышленных системах, которые надо защищать
Инженер	Знает все о работе ключевых систем, используемых в организации и промышленной безопасности	Не знает ничего об информационной безопасности
IT-специалист	Может помочь в части выстраивания инфраструктуры или настройки ПО	Но он тут по большому счету ни при чем!
Инженер-безопасник		

Где искать кадры?

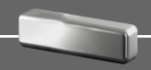
Специалист по ИБ	Знает все про вопросы информационной безопасности	Не знает ничего о промышленных системах, которые надо защищать
Инженер	Знает все о работе ключевых систем, используемых в организации и промышленной безопасности	Не знает ничего об информационной безопасности
IT-специалист	Может помочь в части выстраивания инфраструктуры или настройки ПО	Но он тут по большому счету ни при чем!
Инженер-безопасник	Тот самый специалист по обеспечению безопасности объектов КИИ. Тот кто нам нужен!	

Где искать кадры?



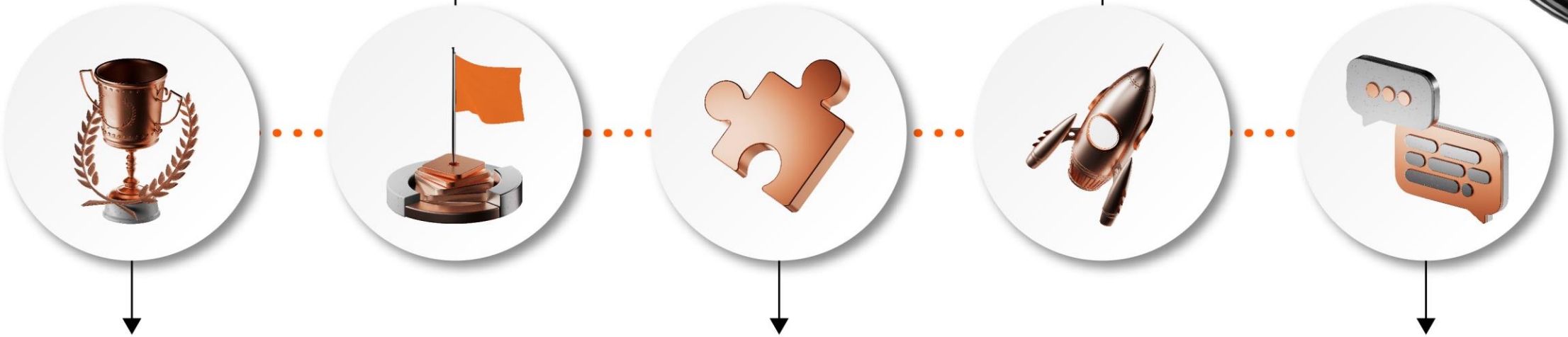
Специалист по ИБ	Знает все про вопросы информационной безопасности	Не знает ничего о промышленных системах, которые надо защищать
Инженер	Знает все о работе ключевых систем, используемых в организации и промышленной безопасности	Не знает ничего об информационной безопасности
IT-специалист	Может помочь в части выстраивания инфраструктуры или настройки ПО	Но он тут по большому счету ни при чем!
Инженер-безопасник	Тот самый специалист по обеспечению безопасности объектов КИИ. Тот кто нам нужен!	Зачастую не существует в природе

Где искать кадры?



Специалист по ИБ	Знает все про вопросы информационной безопасности	Не знает ничего о промышленных системах, которые надо защищать
Инженер	Знает все о работе ключевых систем, используемых в организации и промышленной безопасности	Не знает ничего об информационной безопасности
IT-специалист	Может помочь в части выстраивания инфраструктуры или настройки ПО	Но он тут по большому счету ни при чем!
Инженер-безопасник	Тот самый специалист по обеспечению безопасности объектов КИИ. Тот кто нам нужен!	Зачастую не существует в природе

Резюме



Выбор подхода всегда только **за субъектом КИИ**

Чтобы сделать верный выбор необходимо **грамотно сформировать комиссию** по категорированию.

Специалисты с экспертными знаниями о ваших системах – главные кадры в задачах функционирования объектов КИИ. Не потеряйте их!

Переобучение и повышение квалификации специалистов – залог успешности выполнения задач, связанных с КИИ

Нет своих специалистов или компетенций – **обращайтесь к профессионалам.** Это позволит избежать существенных ошибок, а в последствии сэкономить бюджет, время и ресурсы.

AKTIV.
CONSULTING

БЛАГОДАРЮ
ЗА ВНИМАНИЕ!

Ольга Копейкина

Ведущий консультант

kopeikina@aktiv.consulting