AKTIV.
CONSULTING

Практика внедрения операционной надежности: взаимодействие с поставщиками

Александр Моисеев

Ведущий консультант
по информационной
безопасности

О чем сегодня поговорим:

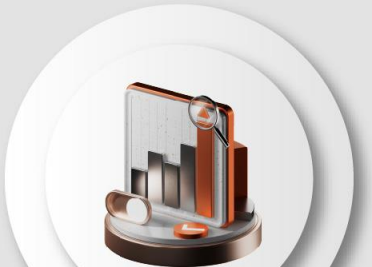
Основные сложности
защиты цепочки
поставок в КО и НФО

Рекомендации
по реализации
требований

Основные сложности защиты цепочки поставок в КО и НФО

1.1 Востребованные услуги поставщиков в финансовой отрасли

1.2 Основные цепочки поставок



1.3 Действующие нормативные требования

1.4 Управление риском реализации угроз

1.5 Управление риском технологической зависимости

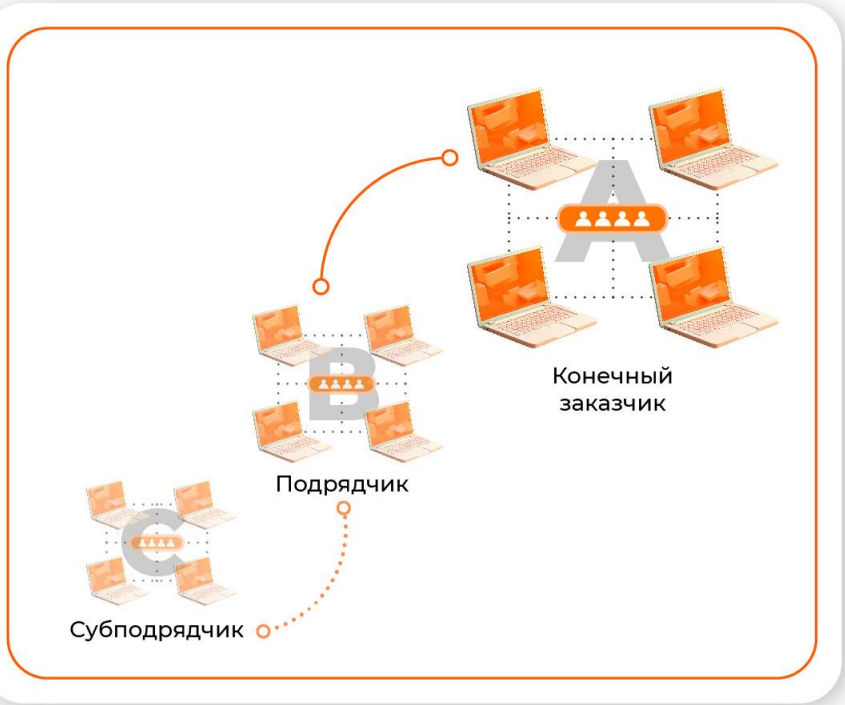
1.1 Востребованные услуги поставщиков в финансовой отрасли

Сервисы	КО	НФО
1. Телематические услуги		
подключение к сети Интернет	+++	+++
2. ЦОД и облачные услуги		
co-location	++	+
аренда ресурсов	+	+++
managed-сервисы	+	+++
3. Информационные системы		
ДБО	+	-
АБС	+	-
Процессинг	+	-
ПОД / ФТ / РОМУ	+++	+++
…		

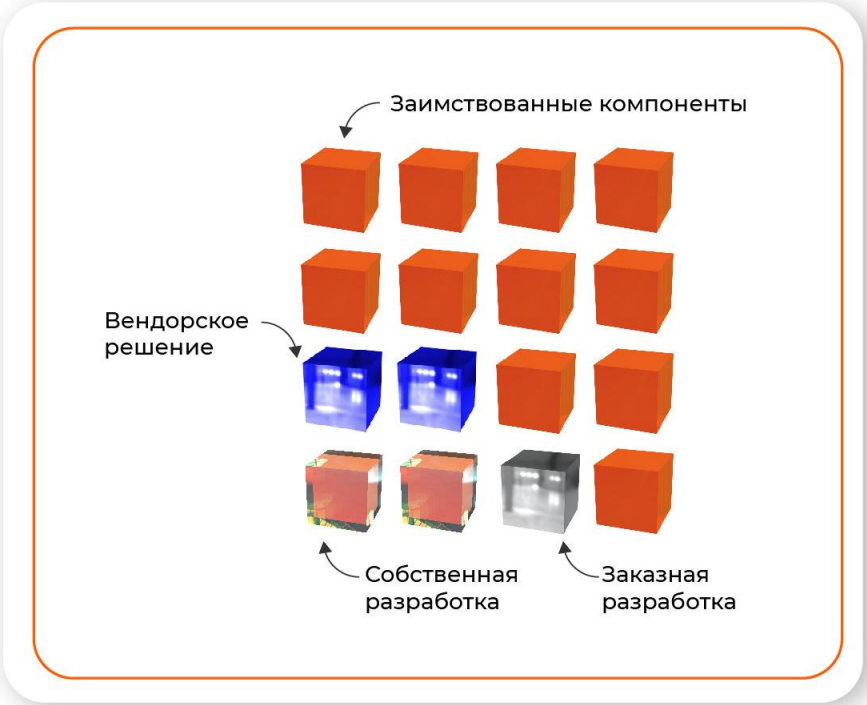
1.2 Основные цепочки поставок

Цепочки поставок

Взаимодействие ИТ-инфраструктур



Взаимодействие программных компонент



1.3 Действующие нормативные требования

787-П / 779-П

МР-7

МР-7 от 21.03.2024 и ГОСТ Р 57580.4, а именно Процесс 4 «Взаимодействие с поставщиками услуг»:

- управление риском реализации угроз при привлечении поставщиков IT-услуг
- управление риском технологической зависимости от поставщиков IT-услуг

Проект стандарта **«Базовый состав орг. и тех. мер при аутсорсинге IT и использовании облачных услуг»**

6679-У / 6680-У

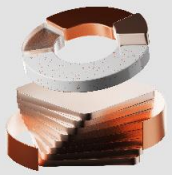
Международная практика:
ISO/IEC 27036, NIST SP 800-161, SCS 9001, NCSC Supply chain security, NIST SP 800-218 SSDF, BSIMM, IEC 62443, OWASP SAMM, PCI SSLC, CNCF Software Supply Chain Best Practices ERM&CK

1.4 Управление риском поставщиков ИТ-услуг

Защита от компьютерных атак

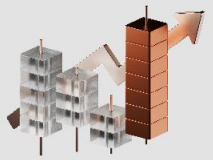
Обеспечение ОН ТП на аутсорсинге:

- NDA и SLA
- альтернативные поставщики



Безопасность цепи поставок:

- оценка репутации и благонадежности
- транспарентность и зрелость процессов
- независимый аудит
- оценка программ безопасности на этапах ЖЦ ОИИ и контроля НДВ



1.5 Управление риском технологической зависимости

Обеспечение ТП на этапах ЖЦ ОИИ

Установление требований ЗИ и ОН к приобретаемым ОИИ

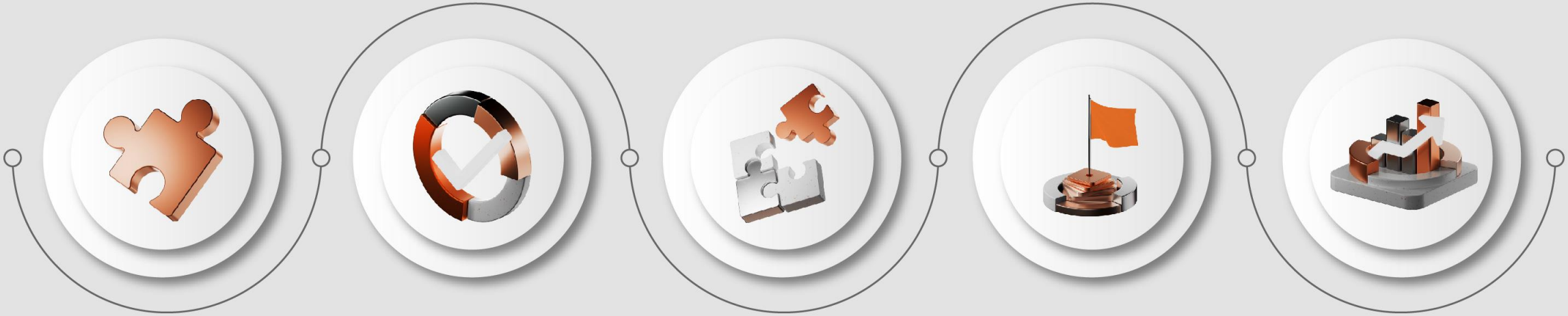
Техническое облуживание ОИИ:

- регистрация событий
- проведение ТО в соответствии с ТТ
- тестирование работоспособности после ТО

Контроль удаленной ТП:

- МФА
- регистрация событий
- гарантированное завершение сессий по завершении ТП
- подключение через VPN с ОИИ с аналогичным уровнем защиты

2 Рекомендации по реализации требований



2.1 NDA и SLA

2.2 Лицензионная политика

2.3 Проверка контрагентов

2.4 Укрепление ОИИ

2.5 Управление требованиями

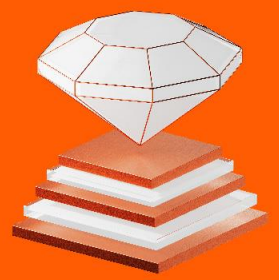
2.1 NDA и SLA *(1/2)*

NDA

1. Классификация и маркировка
2. Обязательства работников
3. Доступ и аудит
4. Легальные защищенные каналы обмена информацией

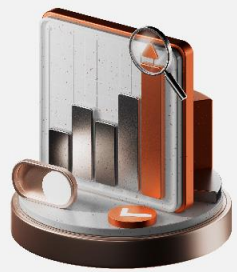
2.1 NDA и SLA *(2/2)*

SLA



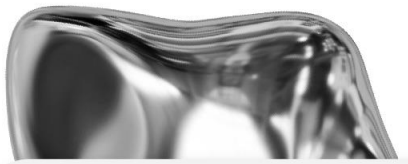
1. Обработка конф. информации
2. Стратегия разрыва отношений
3. Уведомление о привлечении субподрядчиков
4. Порядок возмещения потерь
5. Привлечении к надзорным мероприятиям
6. Регламентация правил удаленного подключения
7. Применение резервных ЦОД
8. Применение СОВ
9. Применение СКЗИ

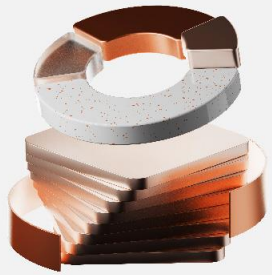
2.2 Лицензионная политика



Применение **вендорского лицензионного ПО**

Фиксация договоренностей при заказной разработке





Анализ применимости компонент «open source»

2.3 Проверка контрагентов

Потенциальный поставщик №1
Потенциальный поставщик №2
. . .
Потенциальный поставщик №N

Поставщик №1

Бывший поставщик №1

Фаза «предконтроля»

Фаза «постконтроля»

Проверка №1
Проверка №2
Проверка №N
Окончательный выбор
Завершение договорных отношений

2.4 Управление требованиями

Потребности
("исходные требования")

Фаза «предконтроля»

Валидация

Требования
("проектные требования")

Верификация требований
(проверка: разработаны ли все требования качественно?)

Верификация требований
(проверка: охватывают ли требования все потребности?)

Информационная система
(к примеру: АБС, ДБО, CRM)

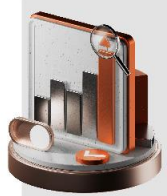
Верификация информационной системы
(проверка: разработана ли ИС в соответствии со всеми требованиями?)

Валидация информационной системы
(проверка: удовлетворяет ли ИС всем потребностям?)

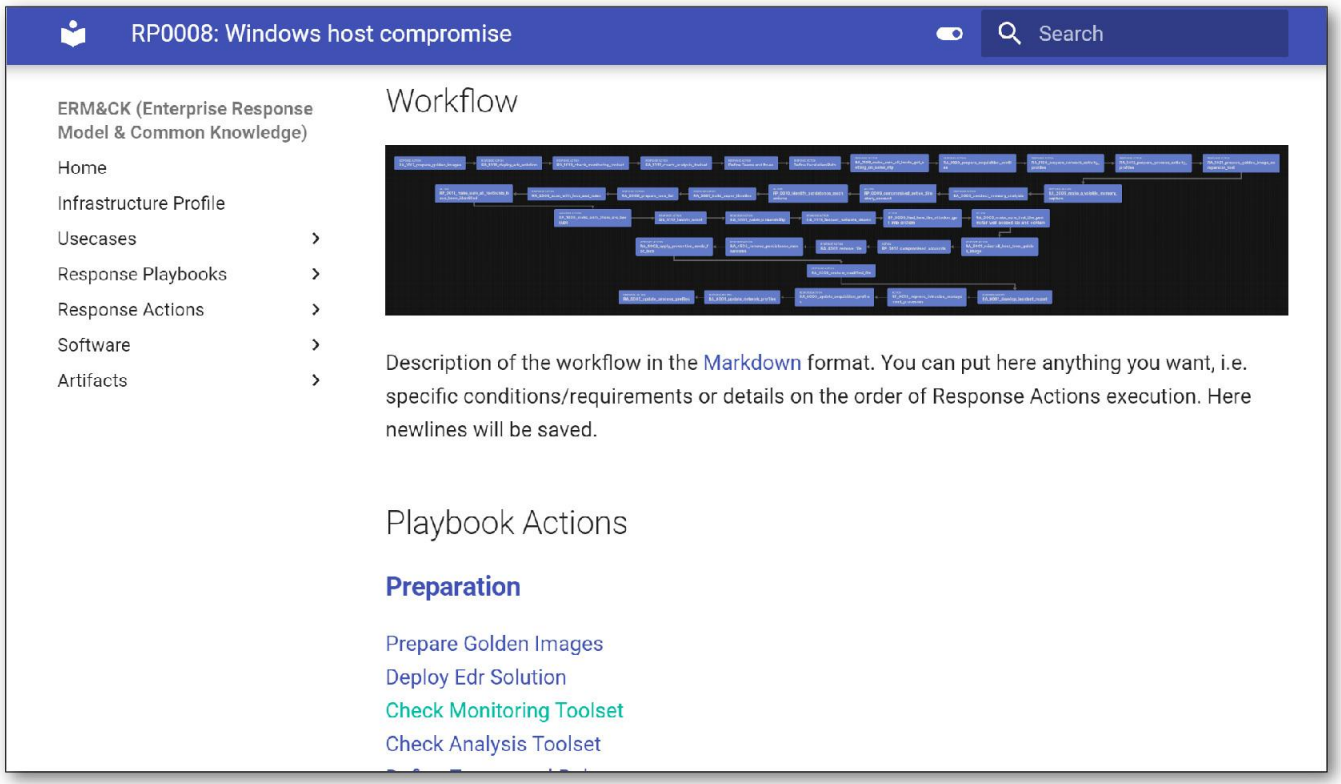
2.3 Укрепление ОИИ:
ИТ-инфраструктура *(1/2)*

ИТ- и ИБ-гигиена, «Hardening»

Зрелость процессов ИБ



Техническое обслуживание ОИИ



2.5 Укрепление ОИИ: ПО (2/2)

Этап	I.Собственная разработка	II. Заказная разработка	III. Вендорская разработка
1. Планирование	I.1.1 Ревью безопасности I.1.2 Формирование требований ИБ	II.1.1 Формирование раздела по ИБ в ТЗ	III.1.1 Анализ имеющихся функций безопасности ПО III.1.2 Доработка ПО вендором по требованиям безопасности
2. Написание кода	I.2.1 Защита исходного кода I.2.2 SCA I.2.3 SAST I.2.4 Базовое обеспечение ИБ среды разработки	II.2.1 Получение выписок из отчетов SAST / SCA	III.2.1 Запрос у вендора выписок из отчетов о SAST / SCA
3. Сборка	I.3.1 Защита пайплайна CI/CD I.3.2 Защита артефактов I.3.3 Безопасное развертывание	II.3.1 Получение лога сборки	–
4. Тестирование	I.4.1 Настройка базовых автотестов I.4.2 Функциональное тестирование I.4.3 DAST / пентест I.4.4 Базовое обеспечение ИБ тестовой среды	II.4.1 Получение выписок из отчетов о тестировании / DAST / пентесте	III.4.1 Запрос у вендора выписок из отчетов о тестировании
5. Развертывание	5.1 Расширенное обеспечение ИБ продовой среды		
	I.5.2 Безопасность контейнеров и оркестраторов	II.5.2 Входной контроль ПО	II.5.3 Проверка всех КС и ЭП
6. Эксплуатация	6.1 WAF		
	6.2 RASP		–
7. Мониторинг	7.1 SIEM		

В качестве резюме

Процессы ОН – это кроссфункциональное взаимодействие, при этом практики одних подразделений, могут обогащать и дополнять практики других

Управление требованиями – важный процесс, при его выстраивании правильным образом – достигается существенная экономия ресурсов

Обязательность внедрения требований ГОСТ Р 57580.4 уже не за горами

Проверка контрагентов – это периодический процесс, во многом схожий с управлением уязвимостями

AKTIV.
CONSULTING

AKTIV.
CONSULTING

БЛАГОДАРЮ
ЗА ВНИМАНИЕ!

Александр Моисеев

Ведущий консультант
по информационной безопасности

moiseev@aktiv.consulting