ALTIRIX GROUP

altirixgroup.com
8 812 716-14-14
info@altirix.ru

МП

Максим Прохоров
Директор по развитию бизнеса

Защита критической информационной инфраструктуры 2021-2022
Тренды и прогнозы

ОСНОВНЫЕ НАПРАВЛЕНИЯ

Информационная безопасность

Законодательство и консалтинг

- Защита персональных данных
- Защита коммерческой тайны
- Защита КИИ
- Защита АСУ ТП
- Расследование инцидентов (форензика)
- Разработка Стратегии ИБ

Создание систем защиты информации

- Аудит
- Проектирование
- Поставка и внедрение СЗИ
- Оценка соответствия
- Сопровождение систем защиты

Анализ защищенности

- Пентест (тестирование на проникновение)
- Штабные киберучения
- Red Team
- Оценка эффективности мер защиты

Решения под ключ

- Управление информационной безопасностью
- Защищенный удаленный доступ
- Криптографическая защита
- Контроль рабочего времени
- План аварийного восстановления (DRP)
- Тренинги, курсы

Информационные технологии

- ИТ-инфраструктура
- Автоматизация бизнес-процессов
- Инфраструктурные решения и сети
- Импортозамещение

Разработка информационных систем

- Блокчейн
- Машинное обучение и нейросети
- DevOps-консалтинг
- Безопасная разработка

НАШИ СЕРВИСЫ:


Пилотирование


Техподдержка


Проектирование


Внедрение


Управляемые сервисы

НАШ ОПЫТ

200+
Выполненных проектов ИБ

85+
Аттестованных объектов и систем

350+
Категорированных объектов КИИ

23
Проверки государственными регуляторами

16
Внедрений режима «Коммерческая тайна»

9
Успешных тестов на проникновение

3
Созданных Центра реагирования на инциденты ИБ

20+
Проектов по защите АСУ ТП

КТО СУБЪЕКТ И ГДЕ ВАШ ОБЪЕКТ?

Утвердить до 1 сентября 2019 г. **перечень объектов КИИ подлежащих категорированию +** 1 год **на работы по Категорированию**

ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ 187-ФЗ КИИ

Категорирование объекта КИИ

- Обучение КИИ
- Приказ о создании комиссии
- Методика обследования
- Критические процессы (Акт)
- Перечень объектов КИИ, подлежащих категорированию
- Методика категорирования
- Отчет об обследовании ОКИИ
- Акты категорирования ОКИИ
- Формы направления во ФСТЭК

Обеспечить безопасность значимых объектов КИИ

- Модели угроз и нарушителя
- Техническое задание на создание СБ ЗОКИИ
- Проектирование подсистем безопасности ЗОКИИ
- Пилотирование
- Поставка
- Ввод в эксплуатацию
- Обучение сотрудников

Взаимодействие объекта КИИ с ГосСОПКА

- Субъекты КИИ обязаны организовать взаимодействие с ГосСОПКА
- Информирование НКЦКИ об инцидентах ИБ на объектах КИИ

Зачем нужно?

Соблюдение требований регуляторов (ФСТЭК/ФСБ) *

Повышение уровня защищенности в области КИИ

Что это?

Обеспечение безопасности критической информационной инфраструктуры (КИИ), работа которой жизненно важна для экономики и безопасности **Государства.**

* За нарушение правил эксплуатации объектов КИИ предусмотрены ответственности УК РФ 274.1 / Нарушение требований в области обеспечения безопасности КИИ РФ КоАП 13.12.1

КОМИССИЯ

Директор

- Руководитель ИТ
- Руководитель по безопасности
- Руководители критичных направлений деятельности
- Руководитель подразделения по контролю и учету опасных веществ и материалов
- Представитель юридического отдела
- Руководители отдела автоматизации (АСУ)
- Руководитель подразделения по защите государственной тайне
- Руководитель Отдела по ГО и ЧС, охраны труда, пром. безопасности
- Руководитель финансов и экономики

ОТВЕТСТВЕННОСТЬ

УК РФ

Ст. 274.1. Неправомерное воздействие на КИИ РФ

до 10 лет лишения свободы

Невыполнение требований по безопасности КИИ, в случае наступления инцидента с тяжкими последствиями или их угрозой

до 6 лет лишения свободы

Невыполнение требований по безопасности КИИ, нарушение правил эксплуатации

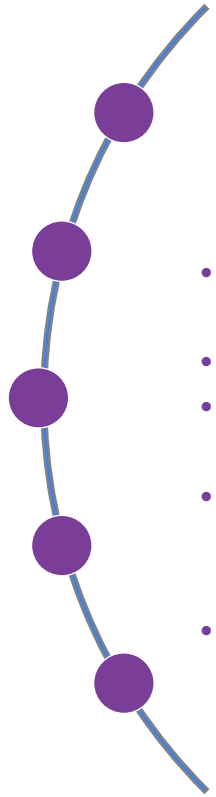
до 5 лет лишение права занимать определенные должности

ч. 3,4,5 ст. 274.1 УК РФ

КоАП РФ

Долж. лица от 10 000-50 000 р.
Юр. лица от 50 000-500 000р.

Нарушение требований в области обеспечения безопасности КИИ РФ



Ответственность возлагается на должностных лиц субъекта КИИ:

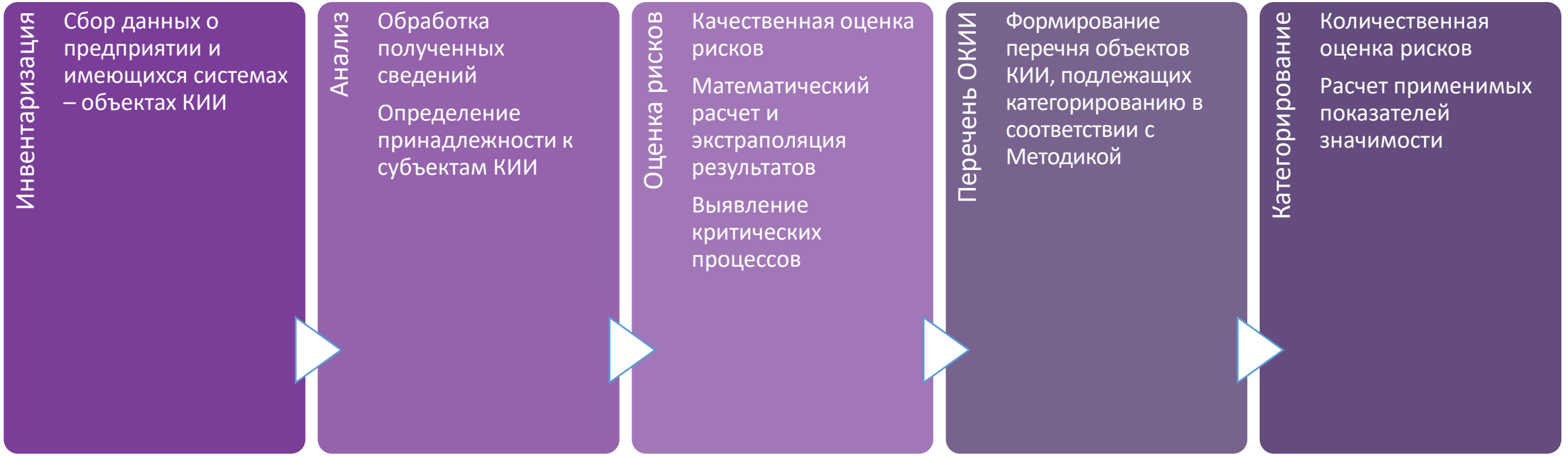
- Руководитель субъекта КИИ
- Уполномоченное лицо
- Лица, эксплуатирующие значимые объекты
- Лица, обеспечивающие функционирование значимых объектов
- Лица, обеспечивающие безопасность значимых объектов

Прокуратура имеет полное право запрашивать любую информацию по исполнению в организации РФ любого закона, в том числе и 187-ФЗ

КАТЕГОРИРОВАНИЕ

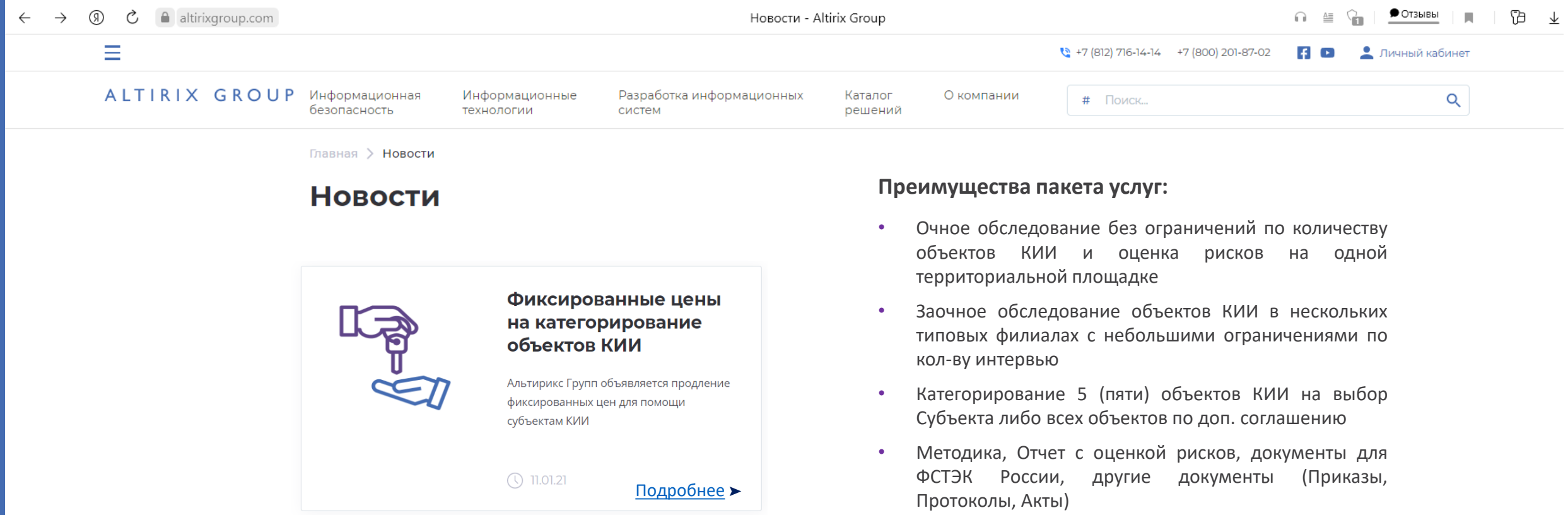
Работы проводятся на основании собственной методики обследования и категорирования объектов критической информационной инфраструктуры, разработанной на основе национальных стандартов и международных практик аудита. Методика позволяет Субъектам беспрепятственно проходить проверки регуляторов.

За 3 года реализации проектов по категорированию объектов КИИ, формы направления сведений в ФСТЭК России, разработанные нашими специалистами, не были возвращены регулятором на доработку – категорирование происходит с первого раза и без ошибок



*** Документирование и согласование с комиссией по категорированию на каждом этапе**

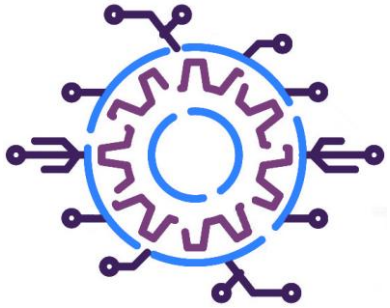
ФИКСИРОВАННЫЕ ЦЕНЫ НА КАТЕГОРИРОВАНИЕ



Преимущества пакета услуг:

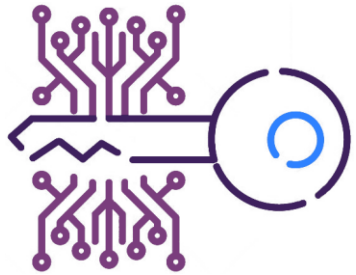
- Очное обследование без ограничений по количеству объектов КИИ и оценка рисков на одной территориальной площадке
- Заочное обследование объектов КИИ в нескольких типовых филиалах с небольшими ограничениями по кол-ву интервью
- Категорирование 5 (пяти) объектов КИИ на выбор Субъекта либо всех объектов по доп. соглашению
- Методика, Отчет с оценкой рисков, документы для ФСТЭК России, другие документы (Приказы, Протоколы, Акты)
- Согласование с ФСТЭК России
- Включены командировочные расходы
- Длительность – 60 рабочих дней
- Гарантия – 12 месяцев

ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ



ГИБКОСТЬ РЕАЛИЗАЦИИ

На старте работ определяем способ выполнения каждого проекта для наиболее эффективного достижения целей исходя из имеющихся временных, финансовых и иных ограничений. Обеспечиваем обоснованный выбор средств защиты за счет практического опыта внедрения и тесного взаимодействия со всеми значимыми представителями на рынке решений по защите информации.



ПРАКТИЧЕСКИЙ ПОДХОД

Обеспечиваем практическую применимость и эффективность создаваемой системы защиты:

- моделирование угроз с учетом цепочек атак (Kill Chain);
- риск-ориентированный подход при оценке угроз;
- оценка результатов методом Дельфи и SWIFT;
- адаптация БДУ ФСТЭК России с учетом MITRE ATT&CK и OWASP.

ФИКСИРОВАННЫЕ ЦЕНЫ НА СОЗДАНИЕ СБ ЗОКИИ

altirixgroup.com Новости - Altirix Group Отзывы

+7 (812) 716-14-14 +7 (800) 201-87-02 Личный кабинет

ALTIRIX GROUP Информационная безопасность | Информационные технологии | Разработка информационных систем | Каталог решений | О компании | Поиск...

Главная > Новости

Новости

Преимущества пакета услуг:

- Очное обследование 1-2 территориальных площадок с ограничением количества единиц оборудования в составе ЗОКИИ (30/100)
- Заочное обследование ЗОКИИ в нескольких типовых филиалах с небольшими ограничениями по кол-ву интервью
- Инвентаризация оборудования и ПО
- Отчет, Модель угроз, Техническое задание, комплект проектной документации, ОРД, Дорожная карта и План мероприятий и ряд других документов
- Включены командировочные расходы
- Длительность – 90-110 рабочих дней
- Гарантия – 12 месяцев

Фиксированные цены на создание систем безопасности ЗОКИИ

Альтирикс Групп предлагает выгодные условия для субъектов КИИ

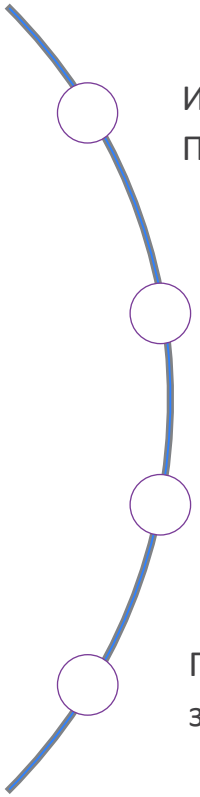
14.06.21

Подробнее ➤

При разработке технических мер по защите информации Альтирикс Групп в приоритетном порядке применяет средства защиты информации, встроенные в программное обеспечение и (или) программно-аппаратные средства значимых объектов (при их наличии). Таким образом в большинстве случаев снижается стоимость владения создаваемой системы безопасности ЗОКИИ.

ИМПОРТОЗАМЕЩЕНИЕ ИБ

Сотрудничество с передовыми российскими разработчиками и **практический опыт перехода с импортных ИТ и ИБ решений** на отечественные позволяют учесть все потребности и ограничения заказчиков при выполнении поставленных задач.



Импортозамещение решений ИТ и ИБ в России определено Постановлением Правительства РФ от 16.11.2015 № 1236

Дополнительные ограничения поставок в связи с санкционным режимом

В России введены Реестр российских программ для ЭВМ (reestr.minsvyaz.ru) и реестр Минпромторга, содержащий перечень российского оборудования

Планируемое расширение ограничений вплоть до запрета использования зарубежных средств защиты для ряда отраслей и предприятий

Преимущественное использование российского ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

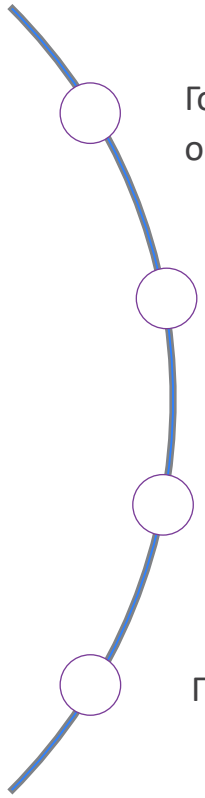
до 1 января 2023 года

Преимущественное использование российского ОБОРУДОВАНИЯ

до 1 января 2023 года

СУБСИДИИ НА ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ КИИ

Предоставление и распределение субсидий из федерального бюджета бюджетам субъектов Российской Федерации на доведение уровня безопасности объектов критической информационной инфраструктуры до установленных законодательством Российской Федерации требований.



Государственная программа Российской Федерации «Информационное общество» дополняется новым приложением № 31

Участниками конкурсного отбора являются субъекты Российской Федерации, реализующие в органах государственной власти субъектов Российской Федерации и (или) подведомственных им учреждениях проекты

Критерием отбора субъектов Российской Федерации для предоставления субсидии является наличие проектов (мероприятий)

Приоритет отдается объектам, имеющим больший охват пользователей

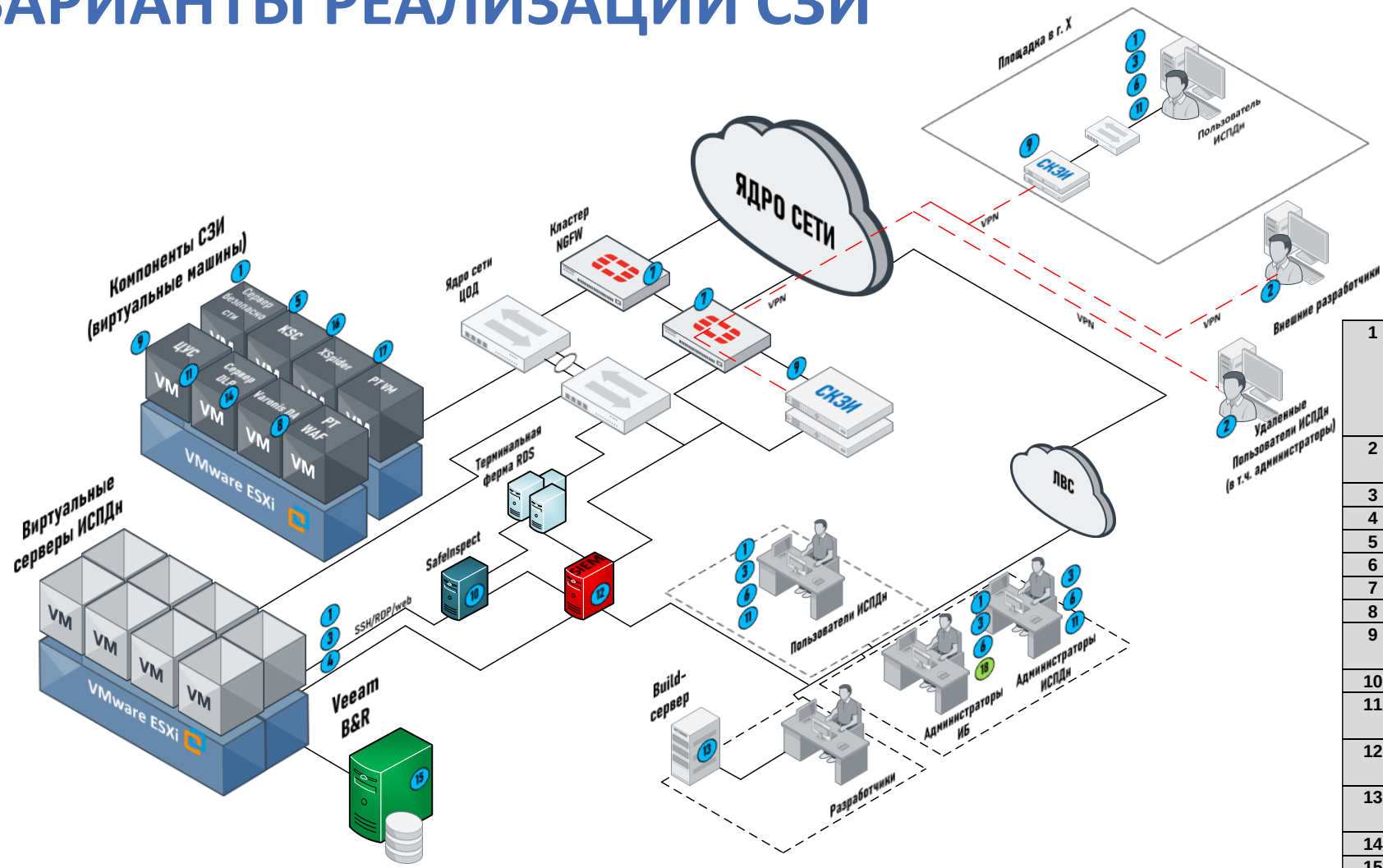
2019 г. Конкурс состоялся

- приняли участие: **36** регионов
- отобрано победителей: **12**
- ВСЕГО: **250 млн рублей**
- в 2020 году 150 млн рублей для объектов КИИ 1 и 2 категории значимости
- в 2021 году 100 млн рублей для объектов КИИ 3 категории значимости.

2021 г. Конкурс отменен

перераспределение бюджетных средств

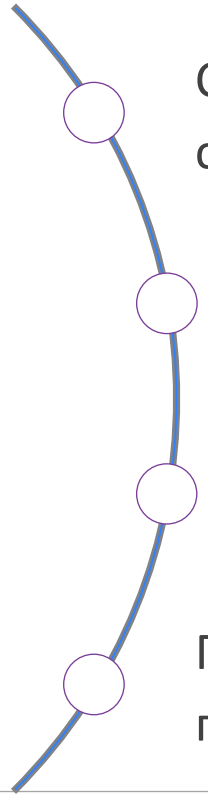
ВАРИАНТЫ РЕАЛИЗАЦИИ СЗИ



1	Встроенные средства защиты ОС
	Сертифицированные ОС
	СЗИ от НСД Secret Net Studio
	СЗИ от НСД ARMlock
	Средства безопасной удаленной работы
2	Aladdin LiveOffice
	Рутокен ЭЦП Flash
3	Kaspersky Endpoint Security
4	Kaspersky Security для виртуальных сред
5	Kaspersky Security Center
6	Kaspersky EDR
7	FortiGate 401E (IPS Service)
8	PT Application Firewall
9	ПАК "ViPNet Coordinator HW"
	ПАК "Контенент АП"
10	SafeInspect
11	СерчИнформ КИБ
	Infowatch Traffic Monitor Enterprise
12	PT MP SIEM
	RuSIEM
13	PT Application Inspector
	Solar appScreener
14	Varonis DatAdvantage
15	Veeam Backup & Replication
16	Xspider
17	Positive Technologies VM
18	Консоли управления СЗИ

ЗАЩИТА АСУ ТП

В связи с высоким проникновением информационных технологий в промышленную сферу **обеспечение безопасности** автоматизированных систем управления технологическим процессом и защита самих технологических процессов – наиболее **приоритетные направления** для **промышленных предприятий.**



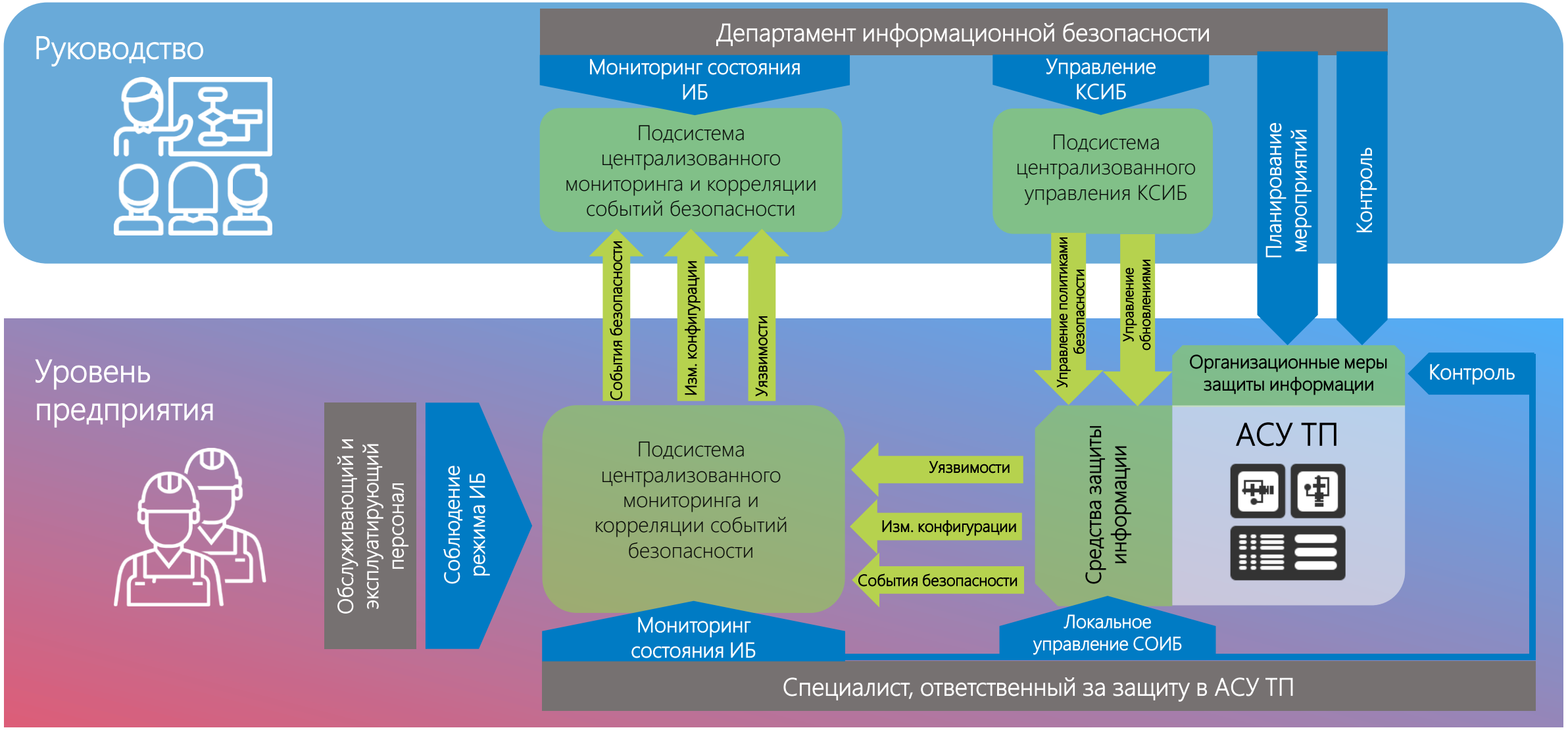
Сотрудничество с вендорами АСУ ТП и тестирование средств защиты для полной совместимости системы защиты и АСУ ТП

Обеспечение непрерывности технологического процесса, разработка Disaster Recovery Plan (DRP)

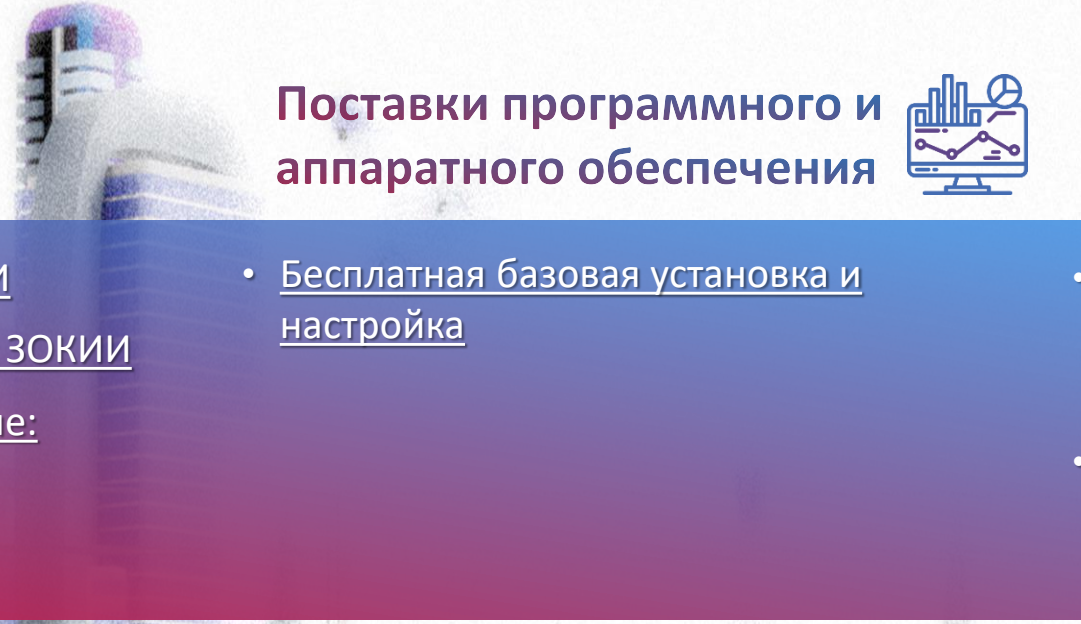
Меры защиты на всех уровнях АСУ ТП: верхний уровень (SCADA), средний уровень (ПЛК) и нижний уровень (датчики и механизмы)

Приоритет использования встроенных механизмов и защитных функций устройств и программного обеспечения АСУ ТП

СХЕМА ОРГАНИЗАЦИОННОЙ СТРУКТУРЫ



ОСОБЕННОСТИ ALTIRIX GROUP



Фиксированные цены

- Категорирование объектов КИИ
- Создание систем безопасности ЗОКИИ
- Тестирование на проникновение:
  - Стартовые пакеты услуг
  - Комплексные пакеты услуг

Поставки программного и аппаратного обеспечения

- Бесплатная базовая установка и настройка

Техподдержка

- Сопровождение по вопросам обеспечения информационной безопасности
- Бесплатная горячая линия по защите КИИ

Официальный сайт | 187-фз.рф

info@altirix.ru| +7 812 716-14-14