Альтирикс системс

Категорирование объектов
критической информационной инфраструктуры

ОСНОВНЫЕ ПОНЯТИЯ 187-ФЗ

- **Субъект КИИ –** организация (орган власти, юридическое лицо, ИП), которому принадлежит хотя бы одна информационная система (ИС), информационно-телекоммуникационная сеть (ИТС), автоматизированная система управления (АСУ), функционирующая в одной из установленных отраслей *
- **Объект КИИ –** ИС, ИТС, АСУ субъекта КИИ

- Здравоохранение
- Наука
- Транспорт
- Связь
- Энергетика и ТЭК
- Финансовый сектор
- Атомная энергетика
- Оборонная отрасль
- Ракетно-космическая
- Горнодобывающая промышленность
- Металлургическая промышленность
- Химическая промышленность

* Принадлежность к отраслям определяется на основании кодов ОКВЭД, Устава и лицензий предприятия

ОСНОВНЫЕ ЗАДАЧИ СУБЪЕКТА КИИ

- **Создать комиссию** по категорированию объектов КИИ
- Установить основные процессы в рамках видов деятельности

- Определить объекты КИИ, подлежащие категорированию
- Направить **Перечень объектов КИИ** во ФСТЭК России

- Определить **категории значимости** объектов КИИ из Перечня
- Направить во ФСТЭК России **результаты категорирования**

- **Информирование НКЦКИ** об инцидентах на объектах КИИ
- Создать Систему безопасности значимых объектов КИИ

* Национальный координационный центр по компьютерным инцидентам создан приказом ФСБ России

СОЗДАНИЕ КОМИССИИ

- Определить **состав членов комиссии** по категорированию объектов КИИ в соответствии с п. 11 **Правил категорирования**, утвержденных Постановлением Правительства РФ от 08.02.2018 № 127
- Разработать **Положение о комиссии** по категорированию объектов **КИИ**
- **Создать комиссию** по категорированию объектов КИИ
- Подготовить план и методику работ по определению и категорированию объектов КИИ

ФОРМИРОВАНИЕ ПЕРЕЧНЯ ОБЪЕКТОВ КИИ

- **Определить** управленческие, технологические, производственные, финансово экономические и (или) иные **процессы**
- Выявить **критические процессы**
- Определить **объекты КИИ**, которые обрабатывают информацию в рамках критических процессов и (или) осуществляют управление, контроль или мониторинг таких процессов
- Сформировать и направить во ФСТЭК России **Перечень объектов КИИ**, подлежащих категорированию

КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ КИИ

1. Комиссия
2. Перечень
3. **Категорирование**
4. Реализация

- Провести **анализ угроз безопасности** для объектов КИИ из Перечня
- Разработать **методику подсчета** (оценки) показателей критериев значимости для объектов КИИ
- Рассчитать **значение показателей** критериев значимости для каждого объекта КИИ
- Присвоить объектам КИИ **категории значимости** или принять решение об отсутствии такой необходимости
- Оформить **акты категорирования** объектов КИИ
- Направить во **ФСТЭК России сведения о результатах** присвоения категорий значимости

ВЫПОЛНЕНИЕ ОБЯЗАННОСТЕЙ СУБЪЕКТА КИИ

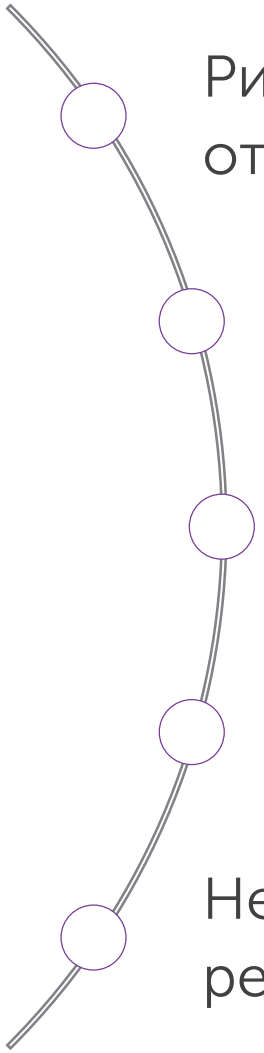
1. Комиссия
2. Перечень
3. Категорирование
4. **Реализация**

- Разработать регламент по реагированию на компьютерные инциденты и **обеспечить информирование НКЦКИ**

В случае наличия значимых объектов КИИ:

- Разработать **модели угроз** и нарушителя
- Обеспечить взаимодействие с **ГосСОПКА**
- Создать **Систему безопасности** значимых объектов КИИ
- Разработать **План реагирования** на компьютерные инциденты
- Обеспечить регулярное **тестирование защищенности** и **анализ уязвимостей** значимых объектов КИИ
- Организовать периодическое **обучение персонала**

В ЧЕМ СЛОЖНОСТЬ



Риск некорректного выполнения требований законодательства в силу отсутствия опыта и методических документов

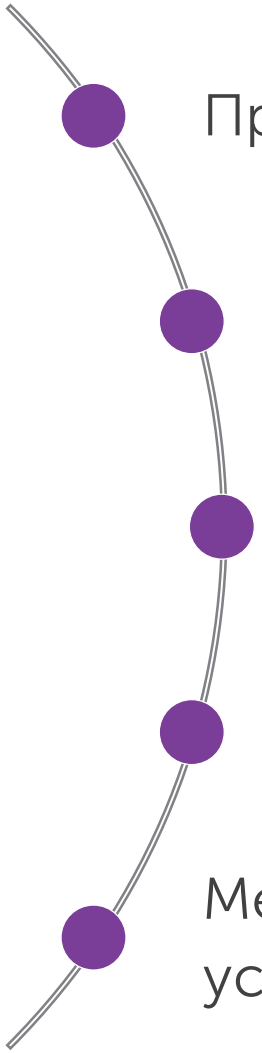
Высокая загруженность специалистов ИБ и отсутствие компетенций в новой предметной области

Недостаточная информированность членов Комиссии о структуре, функционировании и эксплуатации объектов КИИ

Риск уголовной ответственности за инциденты ИБ на объектах КИИ

Недостаточность или отсутствие обоснований для принятия Комиссией решений по определению и категорированию объектов КИИ

ПРЕИМУЩЕСТВА АЛЬТИРИКС СИСТЕМС

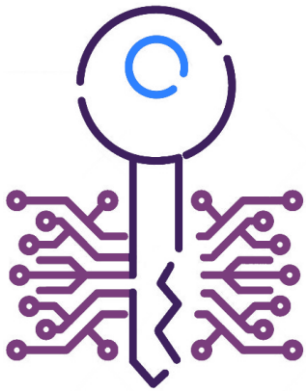


- Практический опыт категорирования и защиты объектов КИИ
- Опытная команда сертифицированных аудиторов и инженеров ИБ
- Наличие всех необходимых лицензий ФСТЭК и ФСБ России
- Гарантированное достижение требуемых результатов в срок
- Методика категорирования и оценки рисков для объектов КИИ, успешно реализованная на предприятиях различных отраслей

НАШ ПОДХОД К РЕАЛИЗАЦИИ ПРОЕКТОВ ПО 187-ФЗ

СОБСТВЕННАЯ МЕТОДИКА

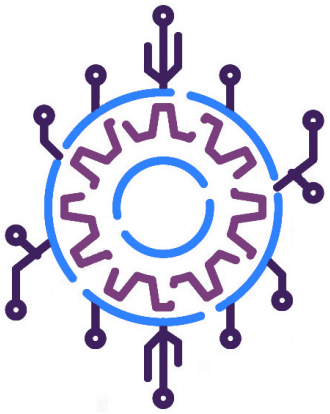
Методика обследования и категорирования выстроена на основе метода Дельфи и SWIFT



ПРАКТИЧЕСКИЙ ПОДХОД

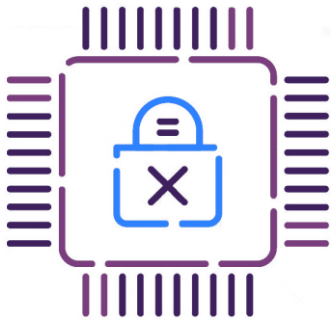
Моделирование угроз производится с учетом цепочек атак (Kill Chain);

риск-ориентированный подход при оценке угроз



ГИБКОСТЬ РЕАЛИЗАЦИИ

Подбор подхода к достижению целей исходя из имеющихся временных и финансовых ресурсов



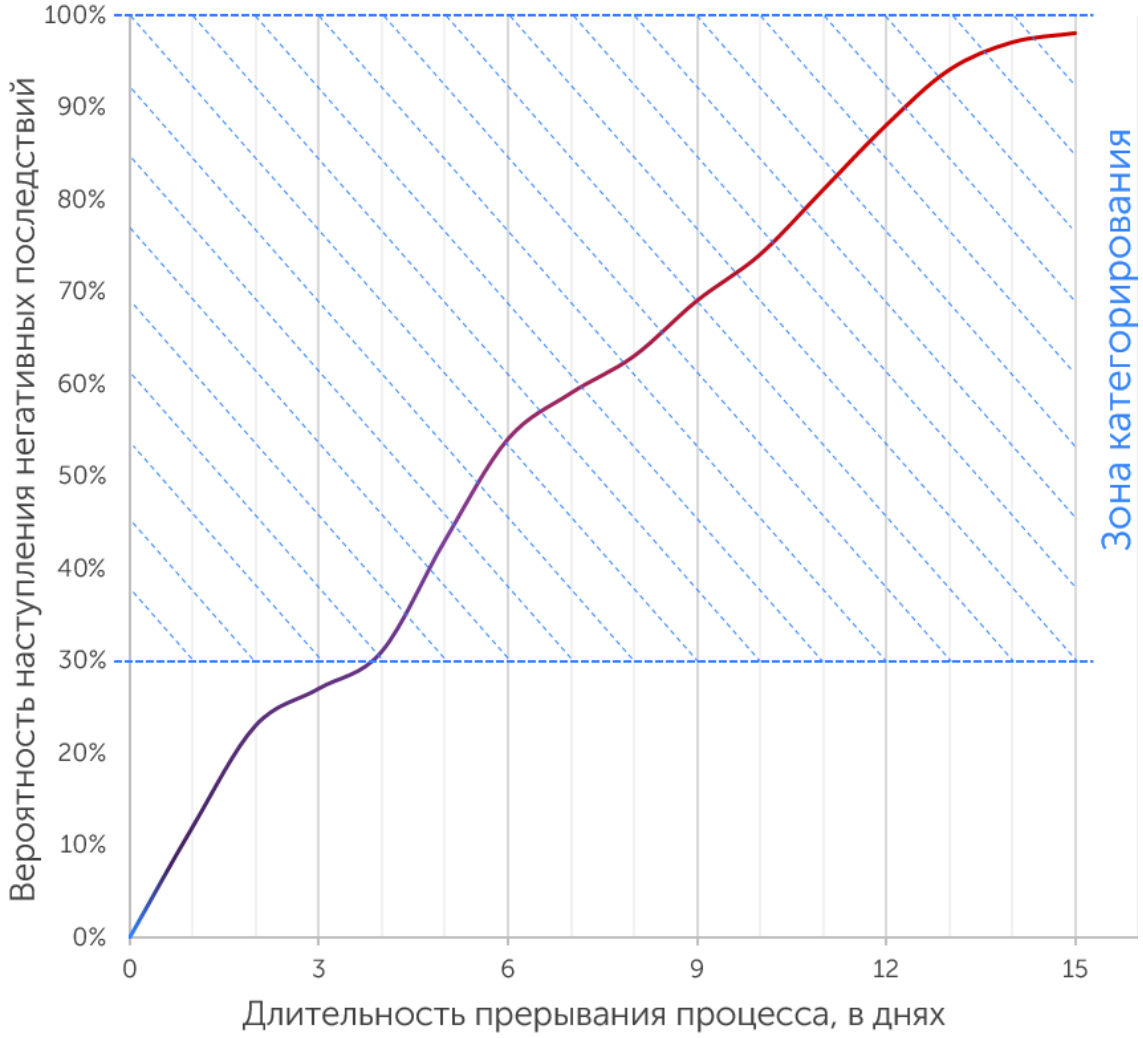
ГАРАНТИРУЕМ КАЧЕСТВО

Несем ответственность за итоговый результат и оказываем помощь при проверках регулирующих органов

МЕТОДИКА ОЦЕНКИ РИСКОВ

Качественная и количественная оценка рисков

- Оценка рисков по ГОСТ Р ИСО/МЭК **31010-2011** «Менеджмент риска. Методы оценки риска»
- Метод **Дельфи** и анализ сценариев методом **SWIFT** для качественной оценки
- **Экстраполирование** результатов анализа с использованием **математической** статистики
- Принятие **обоснованных решений** комиссией на основе подготовленной информации



НАШИ РЕЗУЛЬТАТЫ

97
Категорированных объектов КИИ

80
Аттестованных объектов и систем

64
Субъекта Российской Федерации

23
Проверки государственными регуляторами

16
Внедрений режима «Коммерческая тайна»

9
Успешных тестов на проникновение

3
Центра реагирования на инциденты ИБ

11
Проектов по защите АСУ ТП

ОСНОВНЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ

Федеральный закон № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры РФ»

Постановление Правительства РФ № 127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»

Постановление Правительства РФ № 162 от 17.02.2018 «Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»

Приказ ФСТЭК России № 235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»

Приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»

Приказ ФСТЭК России № 236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

Приказ ФСБ России № 282 от 19.06.2019 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ»

Приказ ФСБ России № 367 от 24.07.2018 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»

187-ФЗ.РФ | info@altirix.ru | +7 (812) 716-14-14