ДиалогНаука

Системная интеграция и консалтинг в сфере информационной безопасности



Ключевые отрасли

- Финансы
- ТЭК
- Промышленность
- Государственный сектор
- Страхование

с 1992 года
на рынке информационной безопасности

34 года
практического опыта

Компетенции и стандарты

ФСТЭК / ФСБ · PCI DSS · SWIFT · ISO

ДиалогНаука

О компании

Более 30 лет помогаем организациям выстраивать надежную систему информационной безопасности

Оказываем консалтинговые услуги, разрабатываем и поставляем комплексные решения по информационной безопасности, сопровождаем их внедрение и эксплуатацию

Прошли путь от поставщика отдельных программных продуктов до компании, специализирующейся на системной интеграции решений по защите информации

- **Топливно-энергетический сектор**
- **Финансово-кредитный сектор**
- **Страховой сектор**
- **Промышленность**
- **Пенсионное обеспечение**

Соответствие требованиям

помогаем выполнять требования регуляторов и стандартов



Анализ защищенности

оцениваем текущий уровень защиты инфраструктуры и данных



Проектирование защиты

разрабатываем модели угроз, архитектуру и документацию



Внедрение ИБ-решений

поставляем и интегрируем средства защиты информации



Сопровождение

обеспечиваем техническую поддержку, аудит и развитие решений



ДиалогНаука

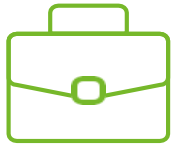
Опыт компании



30+

лет на рынке информационной безопасности

Обладаем уникальной экспертизой и проверенными временем методиками администрирования и сопровождения различных ИБ-систем



170+

ИБ-продуктов в экспертном портфеле Компании

Обладаем глубокой технической экспертизой для успешной реализации комплексных проектов любого уровня сложности



1000+

действующих сертификатов вендоров

Подтверждаем актуальный уровень компетенций наших инженеров напрямую у производителей ПО и систем



ПОЛНЫЙ ПАКЕТ ГОСУДАРСТВЕННЫХ ЛИЦЕНЗИЙ

Гарантируем абсолютную юридическую надежность и безопасность процессов технического сопровождения вашей Компании



Александр Галямин

Директор по сервису

ДиалогНаука

Вебинар: «Жизненный цикл инцидента работоспособности систем защиты информации: от обнаружения до предотвращения»



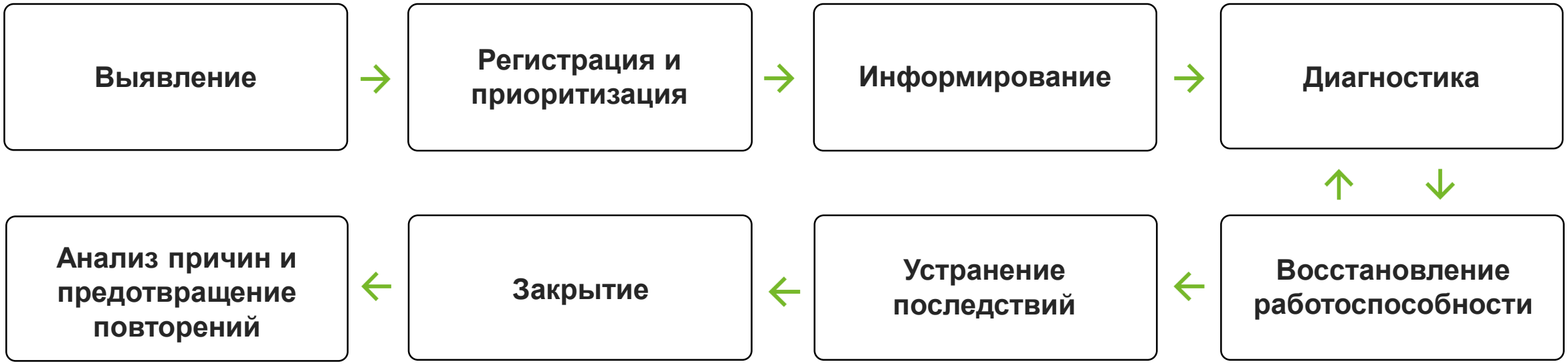
Инцидент работоспособности это незапланированное прерывание сервиса или снижение его качества, которое замечает бизнес.

Каждый час простоя это:

- Прямые потери выручки
- Риск штрафов
- Удар по репутации и доверию пользователей

Инцидент работоспособности - это не хаос, а управляемый процесс с понятными стадиями.

Жизненный цикл инцидента работоспособности систем защиты информации



Стадия 1. Выявление

Откуда приходит сигнал о проблеме:

Пользователи
- Звонки и письма «ничего не работает»
- Узнаем последними, когда ущерб уже идет

Системные администраторы
- Замечают по косвенным признакам или при плановых проверках
- Быстрее пользователей, но зависит от человека и времени суток

Профилактические мероприятия
- Обнаружение отклонений в работе системы во время профилактических работ
- Зависит от регулярности проверок

Система мониторинга
- Фиксирует отклонение за секунды, до того, как кто-то успел позвонить
- Работает 24x7, не зависит от людей

Мониторинг сдвигает начало работы с инцидентом с момента жалобы на момент отказа.

Стадия 2. Регистрация и приоритизация

В терминах ITIL регистрация инцидента работоспособности - это обязательная стадия управления инцидентами: каждая заявка получает номер, владельца и историю.
Заявка - это единая точка синхронизации для всех участников.

Что должно быть в заявке:

- Время обнаружения и источник сигнала
- Затронутый сервис и его компоненты
- Симптомы: что именно не работает, у кого, с какого момента
- Влияние на бизнес и срочность, из них складывается приоритет

Кто должен быть в заявке:

- Инициатор (пользователь, мониторинг, администратор)
- Назначенный инженер или группа технической поддержки
- Владелец сервиса

Без фиксации инцидент работоспособности не существует, а значит, им никто не управляет.

Стадия 3. Информирование

Кого оповещаем:

Владелец сервиса: всегда

Пострадавшие подразделения: если инцидент влияет на их работу

Руководство: при высоком приоритете

Смежные команды (инфраструктура, разработка, вендор): если нужно их участие

Что и когда сообщаем:

В начале инцидента:

- Факт инцидента
- Что затронуто
- Что уже делаем

Во время расследования инцидента:

- Статус через согласованные интервалы, даже если новостей нет

В конце:

- Информацию о восстановлении
- Что было причиной
- Какие последствия

Пока инженеры разбираются с проблемой, бизнес должен знать, что происходит.
Молчание технической поддержки воспринимается как бездействие, даже если работа идет.

Стадия 4. Диагностика

Первые диагностические действия:

- Смотрим логи, метрики, события мониторинга
- Проверяем, что менялось недавно: релизы, настройки, инфраструктура
- Двигаемся по цепочке зависимостей от симптома к источнику
- Проверяем гипотезы по одной с фиксированием результата
- Собираем данные для возможной эскалации вендору: диагностические выгрузки, наблюдения, версии ПО

Когда подключаем вендора:

- Симптомы указывают на дефект продукта, а не на настройку
- Исчерпаны шаги из документации и внутренней базы знаний
- При высоком приоритете подключение вендора необходимо делать не в конце, а параллельно с внутренней диагностикой

Вывод диагностики фиксируем в заявке: причина или гипотеза, подтверждение, граница проблемы.

Стадия 5. Восстановление работоспособности

Временные меры:

- Купирование сбойной функции или компонента
- Переключение на резерв, запасной канал, вторую площадку
- Обходной путь: откат версии, перезапуск, отказ от автоматизации
- Ограничение нагрузки

Важно: причина при этом не устранена.
Каждая временная мера получает срок жизни, иначе «временное» становится «постоянным».

Конечное решение:

- Исправление дефекта или ошибки конфигурации
- Патч или обновление от вендора
- Замена отказавшего компонента
- Доработка архитектуры, если причина в ней

Важно: как правило достигается через процесс управления изменениями, с проверкой и планом отката.
Временные меры при этом снимаются, система возвращается в штатный режим.

Временное решение: как можно скорее уменьшить ущерб и вернуть бизнесу возможность работать.
Конечное решение: восстановить штатную работу системы.

Стадия 6. Устранение последствий

Проблема:	Как решаем:
Пока сервис «лежал», часть операций не прошла или записалась наполовину, в системах разные данные.	1. Сверяем данные систем между собой 2. Находим расхождения 3. Восстанавливаем утерянные данные
За время простоя у пользователей остались незавершенные действия, оборванные сессии, неподтвержденные операции, задачи, которые они не смогли довести до конца.	1. Определяем затронутых пользователей 2. Уведомляем их 3. Помогаем завершить или повторить операции
Отключенные функции, обходные пути и ручные процедуры со стадии восстановления никуда не делись.	После конечного решения возвращаем все в нормальный режим и проверяем, что отключенное снова работает.

Сервис поднят, но инцидент работоспособности еще закрывать нельзя.
Необходимо восстановить информационные потоки, операционные циклы и убрать временные решения.

Стадия 7. Закрытие

Подтверждение владельца сервиса:

Восстановление признает не инженер, а владелец сервиса: его сценарии работают, его данные сошлись.

Закрытие заявки:

- Статус
- Итоговая причина
- Примененное решение

Инцидент закрыт не когда инженер сказал «починил», а когда владелец подтвердил — работает, а заявка содержит всю необходимую информацию.

Стадия 8. Анализ причин и предотвращение повторений

Пост-инцидентный разбор:

- Восстанавливаем хронологию по заявке: от первого сигнала до закрытия
- Отделяем первопричину от симптомов
- Смотрим не только «что сломалось», но и «почему процесс это допустил» где не сработал мониторинг, резерв, регламент

Меры предотвращения:

- Технические: устранение первопричины, доработка архитектуры, добавление резервирования
- Наблюдаемость: новые метрики и пороги в мониторинге
- Процессные: инструкции и регламенты по известному сценарию
- База знаний: инцидент превращается в известную ошибку с готовым решением
- Регламентные: введение профилактических работ, нацеленных на превентивное предотвращение проблем

Инцидент без разбора — это отложенный рецидив: ценность устранения инцидента работоспособности не в том, что мы его выполнили хорошо, а в том, что возможность его повторения сведена к минимуму.

Жизненный цикл инцидента работоспособности систем защиты информации VS Техническая поддержка системного интегратора

Выявление →	**Регистрация и приоритизация** →	**Информирование** →	**Диагностика**	
Мониторинг 1-я линия ТП 24x7	Service Desk 24x7	1-я линия ТП 24x7	Углублённый анализ конфигураций Разбор логов	
			↑ ↓	
Анализ причин и предотвращение повторений ←	**Закрытие** ←	**Устранение последствий** ←	**Восстановление работоспособности**	
Консультации Изменение конфигураций	Ревью проблемы и описание решения силами Интегратора	Консультации Изменение конфигураций	Устранение инцидентов силами Интегратора	

Пакеты технической поддержки

Стандарт
Консультируем

- Круглосуточный приём обращений: портал, почта, телефон
- Письменные консультации по настройке и эксплуатации СЗИ
- Совместный разбор инцидентов и логов; действия выполняет заказчик
- Типовые инструкции и руководства
- Мониторинг патчей, оценка критичности, информирование
- Квартальный отчёт по заявкам

Бизнес
Выполняем работы

- Всё из пакета «Стандарт»
- Консультации в реальном времени
- Устранение инцидентов силами исполнителя
- Изменение конфигураций: правила, порты, пользователи, политики, интеграции
- Выезды инженера, профилактика и проверка кластеров
- Непрерывный мониторинг с оповещениями
- Инвентаризация и контроль отклонений конфигураций
- Установка обновлений по запросу
- Индивидуальные инструкции, обновление схем и документации
- Ежемесячная детализированная аналитика

Премиум
Предупреждаем проблемы

- Всё из пакета «Бизнес»
- Восстановление через постоянный авторизованный доступ, обходные решения
- Выезды технического лидера по сложным задачам и критическим инцидентам
- Проактивный анализ аномалий и предупреждение сбоев
- Углублённый анализ конфигураций и оптимизация политик безопасности
- Тестирование обновлений на стендах заказчика перед внедрением
- Персональная отчётность с метриками и рекомендациями
- Предложения по развитию и оптимизации
- Выделенный Technical Lead и чат с командой (с фиксацией в Service Desk)

Консультации и инструкции
Действия по устранению проблемы выполняет заказчик

Работы силами инженеров
Исполнитель устраняет инциденты и меняет настройки

Проактивное сопровождение
Исполнитель предупреждает сбои и ведёт сложные задачи

Логика пакетов: Бизнес включает Стандарт; Премиум включает Бизнес.

Условия, объём и SLA — по договору.

Этапы подключения услуг

1. 

Знакомство проектных команд
Проводим стартовую встречу, закрепляем персонального руководителя проекта и утверждаем регламент взаимодействия

2. 

Передача документации и доступов
Принимаем технические материалы по архитектуре и организуем безопасные авторизованные доступы для инженеров

3. 

Подключение к платформе Service Desk
Предоставляем сотрудникам заказчика персональные доступы к системе учета заявок и проводим инструктаж



1 день

4. 

Проведение экспресс-аудита инфраструктуры
Знакомимся с текущим состоянием СрЗИ для обеспечения дальнейших процессов регулярного технического сопровождения



не более 3-х дней

5. 

Старт регулярного оказания услуг
Принимаем СрЗИ на обслуживание, берем в обработку поступающие обращения, активируем параметры SLA

6. 

Предоставление регулярной отчетности
Формируем и направляем прозрачные отчеты о фактически выполненных работах за прошедший период



уже с 5-го дня

Для получения персональной консультации по тематике вебинара и предварительного расчета стоимости услуг

Контакты

Почта

marketing@dialognauka.ru

Телефон

+7 (495) 980-67-76

+7 (499) 670-95-95

Адрес

г. Москва, 1-й Нагатинский проезд, д.10, стр.1, БЦ «Ньютон Плаза»

