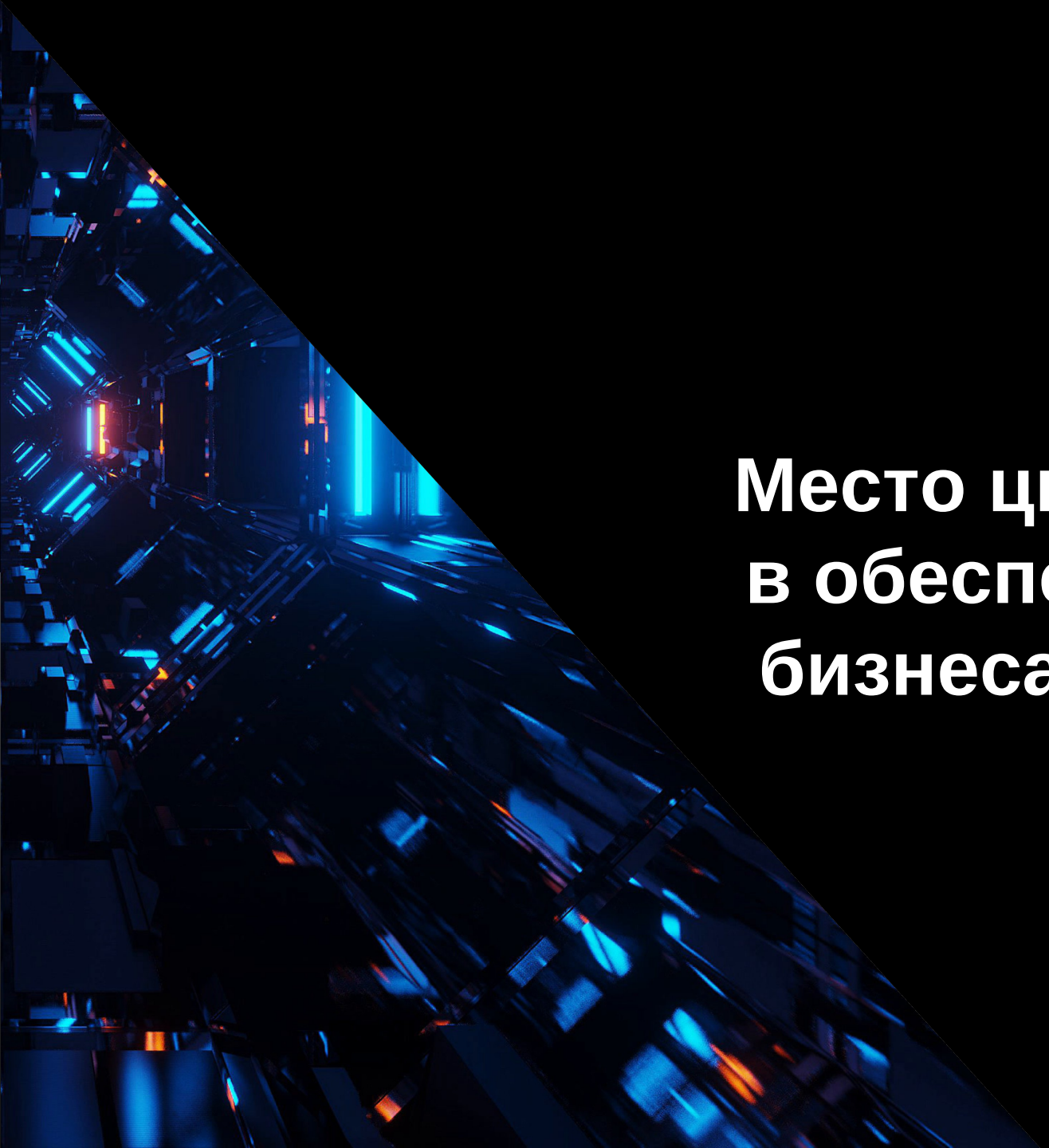


CYBERBIT

Наши технологии – ваше устойчивое развитие

Место цифровой устойчивости в обеспечении непрерывности бизнеса и нюансы реализации

В составе холдинга

Цикада

О КОМПАНИИ

Основана в 2019 году

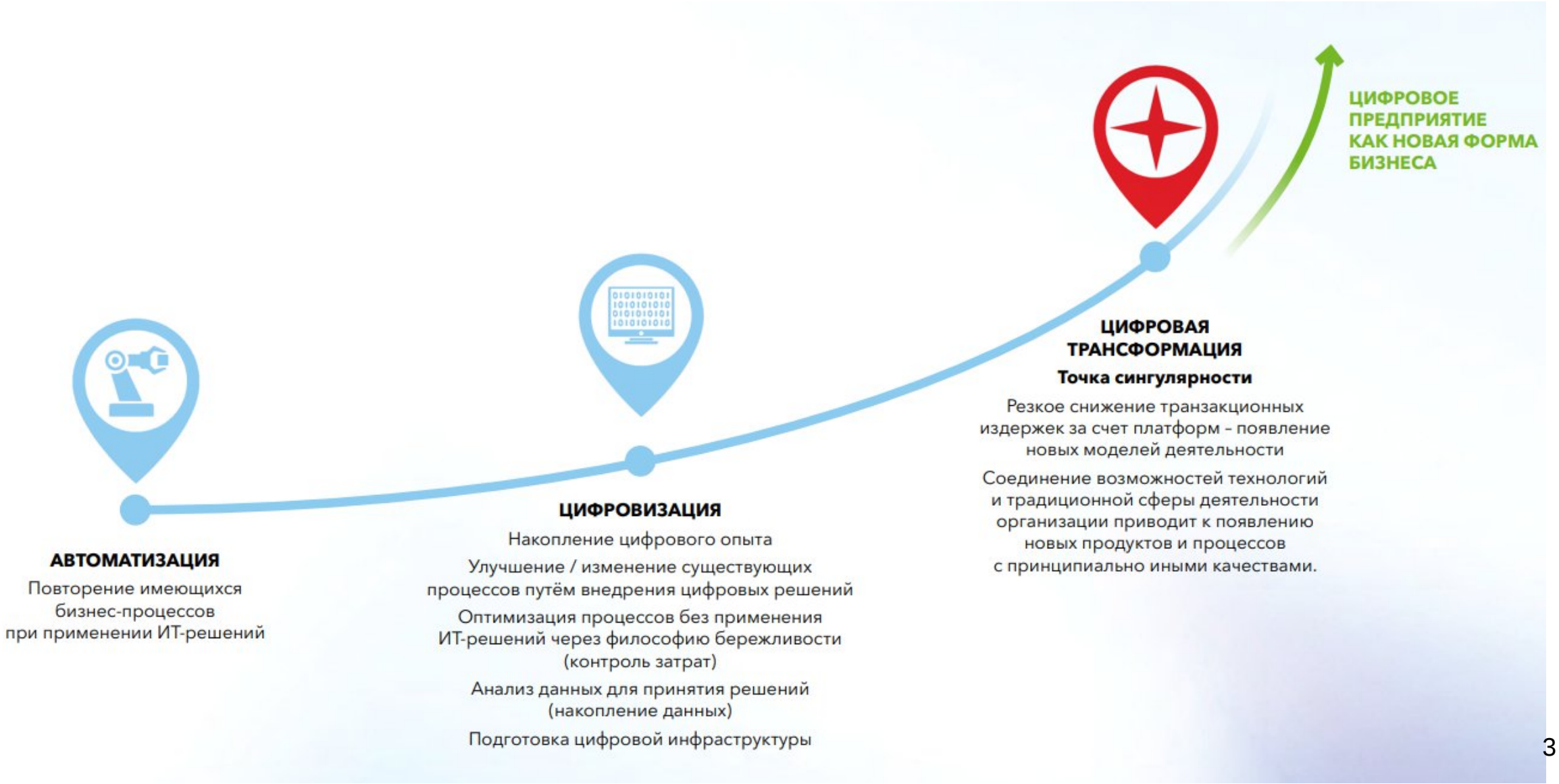
Компетенции

- Экспертиза в сетевой безопасности
- Собственная разработка основного функционала
- Собственная лаборатория функционального и нагрузочного тестирования

COMNEWS AWARDS 2023

победитель номинации
«Лучшее цифровое решение по кибербезопасности»

Тенденции


ЦИФРОВОЕ ПРЕДПРИЯТИЕ КАК НОВАЯ ФОРМА БИЗНЕСА
АВТОМАТИЗАЦИЯ
Повторение имеющихся бизнес-процессов при применении ИТ-решений
ЦИФРОВИЗАЦИЯ
Накопление цифрового опыта
Улучшение / изменение существующих процессов путём внедрения цифровых решений
Оптимизация процессов без применения ИТ-решений через философию бережливости (контроль затрат)
Анализ данных для принятия решений (накопление данных)
Подготовка цифровой инфраструктуры
ЦИФРОВАЯ ТРАНСФОРМАЦИЯ
Точка сингулярности
Резкое снижение транзакционных издержек за счет платформ – появление новых моделей деятельности
Соединение возможностей технологий и традиционной сферы деятельности организации приводит к появлению новых продуктов и процессов с принципиально иными качествами.

Пример целеполагания

ФОКУС МЕНЕДЖМЕНТА НА НЕПРЕРЫВНОСТИ – КЛЮЧ К УСПЕХУ

Ключевой заказчик управления непрерывностью – бизнес

ЗАДАЧА:
ДАНО: ограниченные ресурсы, неограниченные потребности
ЦЕЛЬ: обеспечить непрерывную деятельность компании

Сделать срез AS IS посредством ревизии инфраструктуры и процессов

Приоритизировать наиболее критичные зоны для бизнеса в условиях ограниченных ресурсов

Проработать мероприятия по обеспечению непрерывности деятельности отдельно с ИТ, ИБ и бизнесом в отношении всех критичных ресурсов

мониторинг, тестирование, совершенствование

Пример круга решаемых задач

Пример решения задач непрерывности

Примеры процессов, в которые должна встраиваться ИБ (часть 1)

Планы по формированию комплексной надежности производственных процессов

Элементы		Что требуется
1	**Управление программой надежности**	• Создание единого УК по обеспечению надежности • Выделение инициатив по обеспечению надежности в единый проект, формирование устава проекта • Формирование дорожной карты по реализации проекта
2	**Оценка и снижение рисков**	• Проведение повторных оценок опасностей и технологических рисков после выполнения планов мероприятий • Определение размера остаточных рисков для определения приоритетных направлений разработки стратегий непрерывности в части технологического оборудования
3	**Оценка воздействия простоев на компанию**	• Формирование единой методики расчета простоев • Определение максимально допустимого уровня простоев • Проведение АВБ для всей производственной цепочки газового бизнеса, включая новые объекты • Определение критичного оборудования для новых объектов
4	**Стратегии непрерывности и восстановления**	• Формирование механизма проработки стратегий для критичных бизнес-процессов и ресурсов (единиц оборудования, сотрудников, ИТ, подрядчиков, зданий) с учетом принципов балансировки • Объединение работ по разработке стратегий на всех уровнях
5	**Планы непрерывности бизнеса**	• Определить количество планов для разработки (по результатам АВБ и проработке стратегий) • Организация работы команд восстановления и реагирования для разработки планов • Разработка качественных планов с применением существующей методологии • Постановка разработки планов непрерывности и восстановления на промышленный поток
6	**Планы аварийного восстановления**	• Разработка планов аварийного восстановления критичных единиц оборудования • Разработка планов аварийного восстановления ИТ ресурса

Примеры процессов, в которые должна встраиваться ИБ (часть 2)

Планы по формированию комплексной надежности производственных процессов

Элементы		Что требуется
7	**Кризисное управление и реагирование**	• Организация процедуры каскадирования работы кризисных штабов до уровня дивизионов и объектов • Разработка нормативных документов системы антикризисного управления
8	**Обеспечение ресурсами стратегий непрерывности и восстановления**	• Формирование механизма по обоснованию бюджета на обеспечение стратегий восстановления • Выделение бюджета • Выделение сотрудников
9	**Обучение и повышение осведомленности**	• Обучение операционных команд к устранению инцидентов • Обучение команд восстановления к проведению восстановления • Обучение команд кризисного реагирования • В том числе обучение команд на новых объектах • Повышение интеграции команд, обеспечивающих надежность (технологи, механики, КИП, электрики, эксплуатация и пр.)
10	**Тренировки и тестирование**	• Организация тренировок по восстановлению для обученных команд • Формирование программы тестирования разработанных планов • Организация тренировок по проведению тестирования планов и восстановлению, кризисному реагированию
11	**Постоянное совершенствование**	• Оценка обстоятельств, которые привели к существенному инциденту или кризису • Определение требуемых улучшений и действий • Оценка эффективности разрешения существенного инцидента или кризиса • Обновление планов, включая план кризисного реагирования • Ведение более открытой формы реестра кризисных событий (в определенной мере, достаточной для накопления опыта)
12	**Цифровизация**	Цифровизация процесса управления надежностью • Формирование источников данных по обслуживанию оборудования, включая простои • Внедрение ПО для СУНБ • Внедрение **RCM** • Внедрение системы кризисного реагирования • Внедрение системы мониторинга отказа критичного оборудования

76% промышленных компаний интегрируют информационные и операционные технологии в единую сеть

97% опрошенных сообщили, что атаки на ИТ инфраструктуру предприятия также затронули и ОТ. 47% атак — вымогатели

Источник: АЭЦ INFOWATCH

По результатам мониторинга ИБ-архитектуры 100 отечественных организаций, проведённого ФСТЭК, выяснилось:

89% объектов критической информационной инфраструктуры не имеют минимального уровня защиты.

Источник: D-RUSSIA

«Чаще всего атаки приходились на госсектор, энергетику транспорт связь и образование.»

Замдиректор (НКЦКИ Алексей Иванов
5.02.2025 Инфофорум

https://www.interfax.ru/russia/1006382

«Целями хакеров в 2024 году чаще всего становились компании из отраслей критической информационной инфраструктуры — на них пришлось около 64%»

Red Security
14.01.2025

https://secrets.tbank.ru/novosti/kiberataky-2024/?internal_source=copypaste

Согласно опросу 1800 руководителей ИТ-отделов,

компаниям требуется более 7 месяцев, чтобы восстановиться после киберинцидентов

Под «восстановлением» подразумеваются следующие действия:

- внедрение более жёстких мер безопасности (43% респондентов);
- дополнительное обучение сотрудников (41% респондентов);
- восстановление из резервных копий (38% респондентов);
- коммуникация с заинтересованными сторонами (34% респондентов).

Источник: Fastly

Обеспечение цифровой устойчивости

Лидерство и грамотное управление ИБ как функцией бизнеса

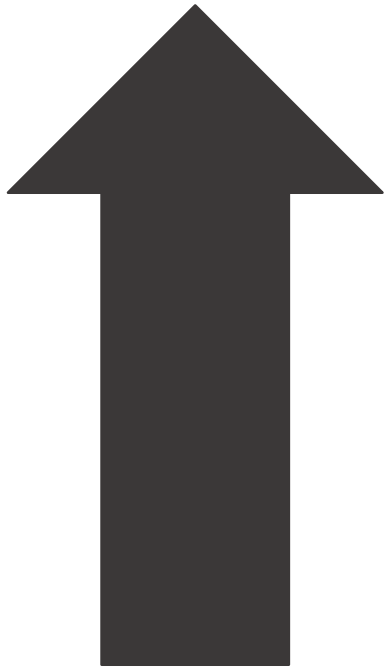
ЛЮДИ

Настройка базовых мер безопасности в ИТ ландшафте и внедрение решений информационной безопасности

ТЕХНОЛОГИИ

Внедрение процессов информационной безопасности в деятельность компании на всех уровнях

ПРОЦЕССЫ



Внедрение технических мер

Внедрение ИБ в бизнес компании

Пример процессов: подсистема ИБ для IOT

Управление	Стратегия и руководство	Руководство программой безопасности
		Обеспечение соответствия внешним требованиям
	Угрозы и риски	Моделирование угроз
		Подход к управлению рисками
	Поставки и внешние зависимости	Управление безопасностью поставок ИТ-компонентов
		Управление зависимостями от внешних ИТ-сервисов
Внедрение	Управление доступом	Управление учётными записями
		Контроль доступа
	Защита активов	Управление активами, изменениями и конфигурацией
		Физическая защита активов
	Защита данных	Модель и политика защиты данных
		Реализация механизмов защиты данных
Укрепление	Уязвимости и обновления безопасности	Поиск и оценка уязвимостей
		Управление обновлениями безопасности
	Ситуационная осведомлённость	Мониторинг и отслеживание событий ИБ
		Поддержание осведомлённости о состоянии ИБ
	Реагирование и восстановление	План реагирования на инциденты безопасности
		Поддержание непрерывной работы и восстановление

iiconsortium

Настройка базовых мер ИБ

- Эшелонированная защита периметра
- Сегментация сетей
- Защита конечных точен
- Анализ трафика внутри сетей
- Анализ и корреляция событий
- Резервное копирование

Лидерство и грамотное управление ИБ

Тренажёры

Бизнес игры

Страт сессии

Тренинги

Для руководителей

- Синхронизация взглядов и действий среди всех руководителей
- Необходимость новых знаний и взглядов на процессы компании
- Сопротивление внедрению изменений со стороны среднего менеджмента и исполнителей

Для руководителей и специалистов ИБ

- Преодоление сопротивления топ-менеджеров при развитии ИБ компании
- Оптимизация отношений ИБ и других функций
- Поиск и привлечение ресурсов внутри компании для решения задач цифровой устойчивости

CBEBIT

Наши технологии – ваше устойчивое развитие

@BUSINESSIIB

В составе холдинга

Цикада

ООО «Корбит»
+7 495 133 26 89
info@corebit.ru
www.corebit.ru