28/03/2024

Информационный доклад

ИНФОТАКТИКА
Мы часть вашей стратегии

ИННОВАЦИОННЫЕ РЕШЕНИЯ И УСЛУГИ ПО ОБЕСПЕЧЕНИЮ **ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

ЮРИЙ СИЛАЕВ
Руководитель отдела НИОКР ГК Инфотактика

ИНФОТАКТИКА
Мы часть вашей стратегии

НАША МИССИЯ

Реализация крупных ИТ-проектов на базе инновационных отечественных телекоммуникационных технологий и решений

НАШИ ЦЕННОСТИ

Профессионализм, надежность, честность, устойчивое развитие

15+
лет на рынке ИТ-решений

390+
экспертов в штате

300+
корпоративных и государственных заказчиков

560+
проектов за 2023 год

80+
регионов — география проектов

ЛИЦЕНЗИИ И СЕРТИФИКАТЫ

ИНФОТАКТИКА
Мы часть вашей стратегии

ФСБ РОССИИ

- **№ 37049 от 11.04.2022**
  на проведение работ, связанных с использованием сведений, составляющих государственную тайну
- **№ 19014/М от 27.07.2022**
  на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны
- **№ 19013/С от 27.07.2022**
  на создание СЗИ, содержащих сведения, составляющие гостайну
- **№ 19242/М от 16.02.2023**
  на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (проведение специальных исследований и специальных проверок для государственной тайны и КИ)
- **№ 16371 Н от 22.12.2017**
  на разработку, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств
- **№ Л001-00105-77/00591149/В от 29.07.2022**
  на выполнение работ по выявлению электронных устройств, предназначенных для негласного получения информации, в технических средствах

ФСТЭК РОССИИ

- **№ 3573 от 15.01.2021**
  на оказание услуг в области защиты государственной тайны
- **№ 3574 от 15.01.2021**
  на создание СЗИ, содержащих сведения, составляющие государственную тайну
- **№ 3383 от 18.08.2017**
  на деятельность по технической защите конфиденциальной информации

МИНКУЛЬТУРЫ

- **№ Л040-00103-00/00670217 от 21.08.2023**
  на осуществление деятельности по сохранению объектов культурного наследия

РОСКОМНАДЗОР

- **№ Л030-00114-77/00648112 от 25.04.2023**
  на оказание телематических услуг связи
- **№ Л030-00114-77/00621879 от 20.10.2022**
  на оказание услуг связи по предоставлению каналов связи
- **№ Л030-00114-77/00621878 от 20.10.2022**
  на оказание услуг связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации

ЧЛЕНСТВО В СРО

- строительство — до 500 млн руб.
- проектирование — до 300 млн руб.
- инженерные изыскания — до 50 млн руб.

ISO/IEC

- **№ РОСС RU.3795.04ФАБ0.1482/1 от 23.08.2021**
  ГОСТ ИСО/МЭК 27001-2006
  соответствие - система менеджмента информационной безопасности
- **№ РОСС RU.3795.04ФАБ0.1482/1 от 01.09.2023**
  ГОСТ Р ИСО 9001-2015
  соответствие - система менеджмента качества (строительство, проектирование)
- **№ RPS.RU.7485.23 от 02.02.2023**
  ГОСТ Р ИСО 9001-2015, ГОСТ Р ИСО 14001-2016, ГОСТ Р ИСО 45001-2020
  соответствия интегрированной системы менеджмента (строительство, капитальный ремонт)

РОСПОТРЕБНАДЗОР

- **№ 77.01.16.000.М.005104.08.23 от 18.08.2023**
  Санитарно-эпидемиологическое заключение
  на выполнение работ при осуществлении деятельности в области использования источников ионизирующего излучения
- **№ Л034-00111-77/00584935 от 15.04.2021**
  на осуществление деятельности в области использования источников ионизирующего излучения (генерирующих)

ОССЭТ

- **№ ОС-2-У-0828 от 22.03.2023**
  на средства связи (доверенная телекоммуникационная система «Фотон-А»)

НАПРАВЛЕНИЯ БИЗНЕСА

ИНФОТАКТИКА
Мы часть вашей стратегии

ОБЕСПЕЧИВАЕМ ЗАЩИТУ ИНФОРМАЦИИ НА ВСЕХ УРОВНЯХ

- Разработка и производство средств защиты информации
- Защита информации, содержащей сведения гостайны
- Защита конфиденциальной информации

ПО КОМПЕТЕНЦИЯМ

- Разработка и производство ПАК
- Специальная интеграция
- Комплексные системы безопасности
- Защита информации
- Специальные телекоммуникации
- Кибербезопасность

ПО ОТРОСЛЯМ

- Госсектор
- Финансовый сектор
- Промышленность
- Телекоммуникации
- Топливно-энергетический комплекс
- Транспорт
- Ритейл

НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ И ЛАБОРАТОРНАЯ БАЗА

ПОСТАВКА ВЫСОКОТЕХНОЛОГИЧНОГО ИТ-ОБОРУДОВАНИЯ

ЦЕНТР ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

ВИДЫ УСЛУГ

ИНФОТАКТИКА
Мы часть вашей стратегии

СИСТЕМНАЯ ИНТЕГРАЦИЯ

- Инфраструктура и ЦОД
- Инженерная инфраструктура
- Сети и телекоммуникации
- Мультимедийные системы
- Комплексная безопасность
- Информационное взаимодействие
- ИТ-аутсорсинг

ПОСТАВКИ ОБОРУДОВАНИЯ

- Персональные компьютеры, моноблоки
- Системные блоки, мониторы
- Материнские платы
- Автоматизированные рабочие места (АРМ)
- Серверы
- Телекоммуникационное оборудование
- Маршрутизаторы

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

- Экспертный консалтинг, аудит и тестирование на проникновение
- Разработка концепции и стратегии развития ИБ
- Проектирование и реализация защищенных объектов информатизации
- Выстраивание процессов кибербезопасности
- Проектирование и внедрение центров мониторинга и реагирования на инциденты ИБ
- Проведение комплексного контроля защищенности и киберучений
- Аттестация объектов информатизации

СЕРВИС

- Техподдержка и сервис ИТ-инфраструктуры
- Аудит инфраструктуры
- Настройка и конфигурация оборудования различных вендоров
- Мониторинг оборудования
- Аутсорсинг ИТ-услуг
- Выполнение комплексных проектов, пусконаладочные работы (ПНР), сопровождение
- Контракты с гарантированным временем восстановления
- Расширенная гарантия (обеспечение SLA)

ИНФОТАКТИКА
Мы часть вашей стратегии

СИСТЕМНАЯ ИНТЕГРАЦИЯ

ГОСУДАРСТВЕННЫЙ ЗАКАЗЧИК (гостайна)

Задача: проектирование и строительство резервного ЦОД

Объем проекта:
180 стоек

Сроки реализации:
2019-2021 гг.

Решение: строительство резервного ЦОД с нуля, обеспечивающего 100% резервирования существующей инфраструктуры; поставка шкафов, ИБП для обеспечения отказоустойчивости, организация системы электроснабжения, кондиционирования и вентиляции, системы автономного газового пожаротушения

ФЕДЕРАЛЬНАЯ ТАМОЖЕННАЯ СЛУЖБА

Задача: создание и быстрое введение в эксплуатацию ЦОД, минимизация расходов

Объем проекта:
30+ территориально-распределенных объектов

Сроки реализации:
январь-июнь 2021 г.

Решение: поставка автономных микро-ЦОД, обеспечивающих стабильное бесперебойное питание и температурно-влажностный режим, не уступающие характеристикам «большим» ЦОД. Цикл производства — около трех месяцев, сроки развертывания — несколько рабочих дней за счет модульной конструкции

ГУП «Мосгортранс»

Задача: организация систем безопасности в соответствии с требованиями законодательства

Объем проекта:
25+ территориально-распределенных объектов

Сроки реализации:
2019-2020 гг.

Решение: проектирование и построение систем охранно-тревожной сигнализации (СОТС), контроля и управления доступом (СКУД), видеонаблюдения, включая подсистемы охранного телевидения, интеллектуального видеонаблюдения и видеозаписи, связи, приема и передачи информации и аудиозаписи, оповещения и громко-говорящей связи, сбора и обработки информации

ПАО «Газпром»

Задача: проектирование и строительство региональной сети передачи данных

Объем проекта:
87+ территориально-распределенных объектов

Сроки реализации:
2020-2023 гг.

Решение:
Проектирование региональных систем передачи данных ООО «Газпром добыча Астрахань» и ООО «Газпром добыча Ямбург». Поставка шкафов, ИБП для обеспечения отказоустойчивости, организация системы электроснабжения, кондициони-рования и вентиляции. Проведение строительно-монтажных и пуско-наладочных работ

ИНФОТАКТИКА
Мы часть вашей стратегии

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЭНЦ

НМИЦ эндокринологии

Решение: построение единого защищенного информационного пространства

ГАЗПРОМБАНК

БАНК АО «ГПБ»

Решение: создание системы мониторинга и контроля кибербезопасности баз данных непроизводственных сред, внедрение комплексной платформы обеспечения безопасности больших данных

РГАНТД
Российский государственный архив научно-технической документации

РГАНТД

Решение: организация защищенных каналов связи и безопасного доступа в сеть Интернет

Мосгортранс

ГУП «Мосгортранс»

Решение: обеспечение кибербезопасности при построении систем обеспечения транспортной безопасности

Альфа-Банк

АО «АЛЬФА-БАНК»

Решение: модернизация системы мониторинга событий информационной безопасности в процессинговом центре, тестирование технологии подтверждения операций мобильного приложения

MOEX НАЦИОНАЛЬНЫЙ КЛИРИНГОВЫЙ ЦЕНТР

НКО АО «НРД»

Решение: создание системы защиты среды виртуализации

ИНФОТАКТИКА
Мы часть вашей стратегии

СЕРВИС

ГОСУДАРСТВЕННЫЙ ЗАКАЗЧИК (гостайна)

Задача: техническая поддержка пользовательской инфраструктуры

Объем проекта:
8 000 АРМ

Сроки реализации: 2020 г.

Решение: двухлетний контракт с возможностью пролонгации на поддержку персональных компьютеров, принтеров с присутствием на территории заказчика для минимизации времени реакции

ФЕДЕРАЛЬНАЯ ТАМОЖЕННАЯ СЛУЖБА

Задача: техническая поддержка сети сетевого оборудования, ВКС и телефонии

Объем проекта:
офисы в 8 регионах

Сроки реализации: с 2022 г.

Решение: двухлетний контракт с возможностью пролонгации на поддержку цифровых и аналоговых АТС, системы ВКС, маршрутизаторов и коммутаторов заказчика

ШЕРЕМЕТЬЕВО
МЕЖДУНАРОДНЫЙ АЭРОПОРТ

АО «МАШ»

Задача: профилактическое обслуживание и ремонт оборудования и систем противопожарной защиты

Объем проекта:
три терминала, межтерминальный переход и комплекс прилегающей территории

Сроки реализации:
с 2021 г.

Решение: трехлетний контракт с возможностью пролонгации на обслуживание охранно-пожарной сигнализации, систем оповещения, дымоудаления и пожаротушения с присутствием на территории заказчика для минимизации времени реакции

ЗАКАЗЧИКИ

ИНФОТАКТИКА
Мы часть вашей стратегии

ВТБ

ГАЗПРОМБАНК

Альфа Банк

открытие БАНК

РЖД

ПЭК

Мосгортранс

ЦБДДМО
ЦЕНТР БЕЗОПАСНОСТИ ДОРОЖНОГО ДВИЖЕНИЯ МОСКОВСКОЙ ОБЛАСТИ

НОВОСИБИРСКИЙ ИНСТИТУТ ПРОГРАММНЫХ СИСТЕМ

РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ АРХИВ НАУЧНО-ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ

НАЦИОНАЛЬНЫЙ РАСЧЕТНЫЙ ДЕПОЗИТАРИЙ
ГРУППА МОСКОВСКАЯ БИРЖА

РОСНЕФТЬ

ГАЗПРОМ

РКС
РОССИЙСКИЕ КОСМИЧЕСКИЕ СИСТЕМЫ

ЭНЦ
Эндокринологический научный центр

акадо телеком

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ ТАМОЖЕННАЯ СЛУЖБА, ЦЕНТРАЛЬНОЕ ТАМОЖЕННОЕ УПРАВЛЕНИЕ

ФЕДЕРАЛЬНАЯ СЛУЖБА ОХРАНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ФИНАНСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ИНОСТРАННЫХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО КУЛЬТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОТАКТИКА
Мы часть вашей стратегии

Материально-техническое обеспечение:

СОБСТВЕННАЯ ЛАБОРАТОРИЯ

для проведения специальных проверок и специальных исследований

АТТЕСТАЦИОННЫЙ ОТДЕЛ

Работы, выполняемые в лаборатории

- Проведение специальной проверки по методикам ФСБ России
- Проведение специальных исследований по методикам ФСБ России и ФСТЭК России

Работы, выполняемые на объектах

- Проектирование объектов в защищенном исполнении (автоматизированных систем различного уровня и назначения и выделенных помещений – помещений, предназначенных для ведения закрытых переговоров)
- Аттестация средств и систем на соответствие требованиям по защите информации (автоматизированных систем различного уровня и назначения) и выделенных помещений - помещений, предназначенных для ведения закрытых переговоров)
- Контроль защищенности конфиденциальной информации и информации, составляющей государственную тайну
- Разработка, производство, реализация, установка, монтаж, наладка, испытания, ремонт, сервисное обслуживание технических и программных средств защиты информации

Услуги аттестационного отдела

- аттестация ОВТ (объекты вычислительной техники)
- аттестация выделенных помещений
- аттестация ЗЛВС (защищённая локальная вычислительная сеть)

ЗАЩИТА ИНФОРМАЦИИ. Преимущества

ИНФОТАКТИКА
Мы часть вашей стратегии

- **Собственная лаборатория**
- **Собственное новейшее оборудование**
  (рентгеновская установка, безэховая камера, сборно-разборная конструкция,
  1-й класс экранирования, шумоизолированная зона, безэховая перегородка,
  всё для проведения методов АРТМ)
- **Собственная доставка техники** со склада клиента до лаборатории и обратно
- **Склад ответственного хранения** – возможность хранение оборудования до того момента,
  как оно понадобится заказчику
- **Работы «под ключ»** начиная от закупки заканчивая доставкой
- Возможность поставки проверенной **техники собственного производства**
- **Индивидуальный подход** к каждому Заказчику

ИНФОТАКТИКА
Мы часть вашей стратегии

БЕЗОПАСНОСТЬ ПРОМЫШЛЕННЫХ СИСТЕМ

Обеспечение кибербезопасности промышленных объектов
и объектов критической информационной инфраструктуры

Защита предприятия от злоумышленников, блокирование слабых мест в архитектуре производственных технологий

- Аудит кибербезопасности систем промышленной автоматизации
- Создание системы обеспечения кибербезопасности
- Внедрение специализированных средств защиты информации
- Разработка методического обеспечения кибербезопасности
- Комплекс услуг по техническому сопровождению систем кибербезопасности (сервисная поддержка)

КЕЙС ПЕНТЕСТИНГА

ИНФОТАКТИКА
Мы часть вашей стратегии

ПОЛУЧЕН ДОСТУП К «1С: ПРЕДПРИЯТИЕ» С ПРИВИЛЕГИРОВАННЫМИ ПРАВАМИ

МНОЖЕСТВО КРИТИЧЕСКИХ УЯЗВИМОСТЕЙ НА ПОЧТОВОМ СЕРВЕРЕ

НАЛИЧИЕ СЕРВИСОВ УДАЛЕННОГО РАБОЧЕГО СТОЛА (RDP) И ОТСУТСТВИЕ ОГРАНИЧЕНИЯ ПО КОЛИЧЕСТВУ ПОПЫТОК ВВОДА ПАРОЛЯ

ПО РЕЗУЛЬТАТАМ ПЕНТЕСТИНГА

- Захвачены учетные данные пользователей и администраторов домена, имеющих максимальные привилегии;

Получен доступ к:

- персона«1С: Предприятие» /полный/;
- льным данным сотрудников;
- администрированию камер и серверов видеонаблюдения;
- телефонии;
- управлению сетевой архитектурой;
- администрированию сайта.

Общий уровень защищенности «КОМПАНИИ» от атак со стороны внутреннего нарушителя оценивается как НИЗКИЙ.

ФАКТЫ

Более 70% кибератак в мире приходится на целевые атаки.

Самый распространённый способ проникновения в ИТ-инфраструктуру — фишинговые электронные письма сотрудникам и брутфорс

РЕАЛИЗАЦИЯ КСОИБ НА ОБЪЕКТАХ

ИНФОТАКТИКА
Мы часть вашей стратегии

ГК «ИНФОТАКТИКА» С ЦЕЛЬЮ МОДЕРНИЗАЦИИ СИСТЕМЫ ИБ ПРЕДЛАГАЕТ И УСПЕШНО ВНЕДРЯЕТ НА ОБЪЕКТАХ КОМПЛЕКСНЫЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ (КСОИБ).

КСОИБ ЯВЛЯЕТСЯ ВЫСОКОЭФФЕКТИВНЫМ ИНСТРУМЕНТОМ КАК ДОСТИЖЕНИЯ ЗАДАННОГО УРОВНЯ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ, ТАК И ОПЕРАТИВНОГО УПРАВЛЕНИЯ И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЭТАПЫ ПО ВНЕДРЕНИЮ КСОИБ

1. Тестирование на проникновение для оценки уровня защищенности инфраструктуры
2. Аудит инфраструктуры
3. Проектирование КСОИБ
4. Внедрение требуемых решений обеспечения ИБ
5. Разработка методологии управления и контроля ИБ
6. Сопровождение и эксплуатация

НЕДОСТАТКИ

Без внедренной КСОИБ

- Более высокая вероятность успешности компьютерных атак
- Меньше понимания потенциальных рисков
- Более высокая вероятность получить сложности в случае успешной атаки

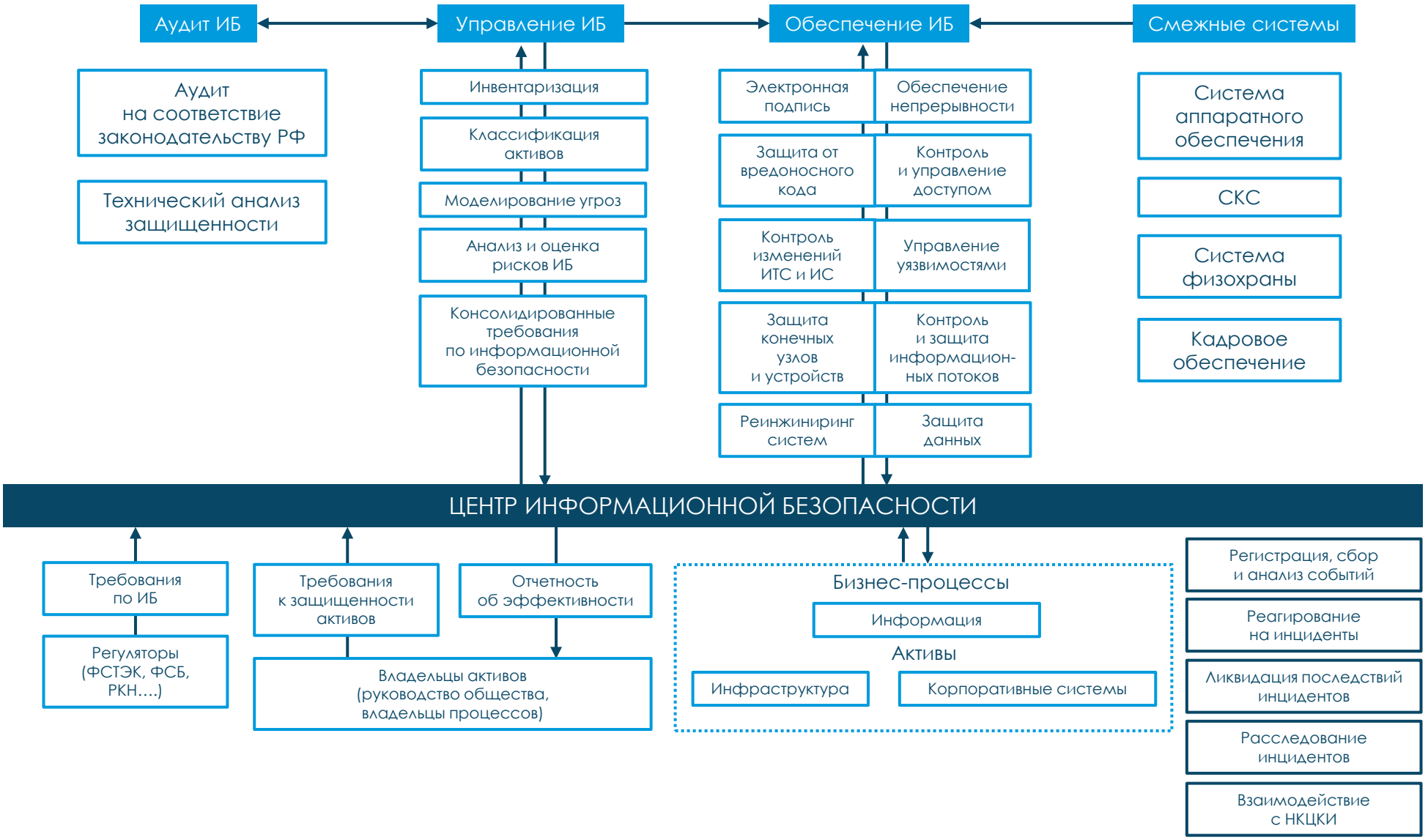
ПРЕИМУЩЕСТВА

С внедренной КСОИБ

- Непрерывность процессов в условиях кибератак
- Понимание рисков информационной безопасности и управление ими
- Больше готовности к внештатным ситуациям
- Более адекватное расследование в случае успешной атаки без «поспешных выводов»

СТРУКТУРА РЕАЛИЗАЦИИ КСОИБ

ИНФОТАКТИКА
Мы часть вашей стратегии



БИОМЕТРИЧЕСКИЕ СКУД

ИНФОТАКТИКА
Мы часть вашей стратегии

БИОМЕТРИЧЕСКАЯ СИСТЕМА КОНТРОЛЯ УПРАВЛЕНИЯ ДОСТУПОМ

1. Невозможность фальсификации вводимых данных
2. Высокая точность распознавания человека
3. Сохранность и надёжность

1. Устанавливаются требования к защите, обработке и хранению биометрических персональных данных
2. Определяются требования по работе с ПДн российских граждан, обеспечивает надлежащий уровень защиты
3. Выделяются общие требования к обработке ПДн

ОТВЕТСТВЕННОСТЬ

149-ФЗ, 152-ФЗ, 572-ФЗ, устанавливают ответственность за нарушение требований данных ФЗ, которая **влечет** за собой **административную, гражданскую и уголовную ответственность**

Пример биометрического терминала компании-партнера

ПО компании-партнера: идентификация и верификация по биометрическим образцам и передача результатов в существующую систему контроля, а также управление доступом для принятия решения

ИНФОТАКТИКА
Мы часть вашей стратегии

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА

Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия

1. Устанавливаются требования к безопасности критической информационной инфраструктуры
2. Устанавливаются обязательные без исключения требования о дополнительных мерах обеспечения безопасности КИИ

ОТВЕТСТВЕННОСТЬ

1. **Указ Президента РФ 250** устанавливает требования для всех без исключения субъектов КИИ и вводит официальный запрет на закупку и использование средств защиты из недружественных стран
2. **187-ФЗ** регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры в целях ее устойчивого функционирования при проведении в отношении неё компьютерных атак
3. **194-ФЗ** дополняет Уголовный кодекс статьей 274.1, которая предусматривает **«За несоблюдение данных нормативно-правовых документов, устанавливаются требования, которые влекут за собой административную гражданскую и уголовную ответственность»**
4. **Ст. 274.1 УК РФ** предусматривает ответственность за неправомерное воздействие на критическую информационную инфраструктуру РФ

ИНФОТАКТИКА
Мы часть вашей стратегии

РАЗРАБОТКА И ПРОИЗВОДСТВО ПАК

CoreBit.NGFW высокопроизводительный многофункциональный межсетевой экран, реализующий функции маршрутизации и фильтрации сетевого трафика в соответствии с заданными правилами на уровне протоколов L2 – L7 с возможностями обнаруживать и предотвращать вторжения.

→ СОБСТВЕННЫЙ МЕХАНИЗМ DPI

- Единая плоскость передачи данных (routing, МЭ, СОВ, MITM)
- Возможность фильтрации с учётом особенностей протоколов

→ НЕ ИСПОЛЬЗУЕМ ГОТОВЫЕ ПОДСИСТЕМЫ (OPEN SOURCE)

- Не используем готовые подсистемы (идентификация, классификация, сборка сессий)

→ НЕ ИСПОЛЬЗУЕМ СТАНДАРТНЫЙ СЕТЕВОЙ СТЕК LINUX

- Все операции в плоскости передачи данных осуществляются в User Space
- Используем аппаратные возможности сетевых адаптеров

→ ОПТИМИЗИРУЕМ РАБОТУ С CPU

- Задачи управления и передачи данных на различных ядрах CPU
- Балансировка сетевой нагрузки в плоскости передачи данных на разных ядрах CPU
- Используем polling ядер CPU

ИНФОТАКТИКА
Мы часть вашей стратегии

ТЕХ.ХАРАКТЕРИСТИКИ

Профиль использования	Интерфейсы и модули	Показатель производительности	Значение
CoreBit.NGFW 250 Для небольших корпоративных сетей (малый бизнес, небольшие филиалы, школы)	- порты GE Rj45 - порт управления MGMT GE RJ45 - порт SYSLOG GE RJ45	▪ Пропускная способность МЭ в режиме статической маршрутизации ▪ Количество одновременных HTTP-подключений ▪ Количество новых HTTP-подключений в секунду МЭ в режиме статической маршрутизации ▪ Пропускная способность в режиме проверки TLS ▪ Пропускная способность в режиме защиты от угроз	▪ до 1100 Мбит/с ▪ до 1 млн. ▪ до 5 000 ▪ до 500 Мбит/с ▪ до 300 Мбит/с
CoreBit.NGFW 500 Для средних корпоративных сетей (средний бизнес, крупные филиалы)	- порты GE SFP и GE Rj45 - порт управления MGMT GE RJ45 - порт SYSLOG GE RJ45	▪ Пропускная способность МЭ в режиме статической маршрутизации ▪ Количество одновременных HTTP-подключений ▪ Количество новых HTTP-подключений в секунду МЭ в режиме статической маршрутизации ▪ Пропускная способность в режиме проверки TLS ▪ Пропускная способность в режиме защиты от угроз	▪ до 4 000 Мбит/с ▪ до 2,5 млн. ▪ до 15 000 ▪ до 1 000 Мбит/с ▪ до 500 Мбит/с
CoreBit.NGFW 2000 Для больших корпоративных сетей (крупный бизнес, интернет-провайдеры)	- порты 10/25 GE SFP28 - порт управления MGMT GE RJ45 - порт SYSLOG GE RJ45	▪ Пропускная способность МЭ в режиме статической маршрутизации ▪ Количество одновременных HTTP-подключений ▪ Количество новых HTTP-подключений в секунду МЭ в режиме статической маршрутизации ▪ Пропускная способность в режиме проверки TLS ▪ Пропускная способность в режиме защиты от угроз	▪ до 20 Гбит/с ▪ до 45 млн. ▪ до 100 000 ▪ до 12 Гбит/с ▪ до 5 Гбит/с
CoreBit.NGFW 5000 Для крупных корпоративных сетей и дата-центров	- порты 40/100 GE QSFP28 - MGMT GE RJ45 - порт SYSLOG GE RJ45	▪ Пропускная способность МЭ в режиме статической маршрутизации ▪ Количество одновременных HTTP-подключений ▪ Количество новых HTTP-подключений в секунду	▪ до 120 Гбит/с ▪ до 20 млн. ▪ до 2 млн.

Примечания

1. Пропускная способность МЭ в режиме статической маршрутизации измерялась при следующих условий:
- тестовый сетевой трафик в конфигурации EMIX с добавлением профилей целевого трафика
(в соответствии с установленными правилами МЭ – 50 000 запрещающих правил уровня фильтрации сервисов);
- статическая маршрутизация (сетевой трафик маршрутизировался между WAN, LAN и DMZ сетями без NAT);
- включенное логирование (за исключением статистики по потокам).
2. Пропускная способность в режиме проверки TLS измерялась с использованием протокола TLS v1.2 и шифрования AES128-SHA256, а также с включенной функцией МЭ.
3. Пропускная способность в режиме защиты от угроз измерялась при включенных функциях МЭ и проверки TLS с установкой 150 правил.

ПАК «СИТО»

ИНФОТАКТИКА
Мы часть вашей стратегии

СИТО NP-1001i

СИТО NP-2001i

Описание продукта

ПАК «СИТО» предназначен для полного или частичного блокирования возможной утечки информации за счет скрытых каналов при передаче информации по каналам связи, защищаемым IP-шифратором.
Скрытый логический канал (СЛК) – это имеющийся в автоматизированной системе механизм, как правило, недекларированный, либо несанкционированно внедренный, функционирование которого может приводить к утечке информации из системы за счет управления характеристиками выходящего из защищаемой сети трафика.

Основные характеристики

ПАК «СИТО» обеспечивает прозрачное объединение TCP/IP сегментов одной или нескольких IP сетей.
Использование изделия обеспечивает канал связи двух и более сегментов сети (число таких сегментов жестко не ограничено, но поддержка большого количества сегментов требует большего количества ресурсов).
Использование адаптивного алгоритма управления интенсивностью потоков данных позволяет ограничить пропускную способность потенциального скрытого канала, а также оптимизировать использование канала связи.

Комплекс предназначен для работы под управлением ОС «Astra Linux Special Edition», РУСБ.10015-17.

АНТИ-БПЛА

ИНФОТАКТИКА
Мы часть вашей стратегии

В январе 2024 года ГК Инфотактика на территории полигона Росгвардии приняла участие в практических занятиях и испытаниях на проверку работоспособности комплексов специальных технических средств противодействия БВС.

Проверка технических характеристик комплексов осуществлялась в соответствии с типовой программой и методикой проведения испытаний специальных технических средств противодействия беспилотным воздушным судам на важном государственном объекте.

По результатам испытаний комплексы показали соответствие заявленным техническим характеристикам.

СПАСИБО
ЗА ВНИМАНИЕ!

ИНФОТАКТИКА
Мы часть вашей стратегии

Москва, ул. Бутлерова, 17
БЦ «NEO GEO»

+7 (495) 481-34-79

info@infotaktika.ru

www.infotaktika.ru