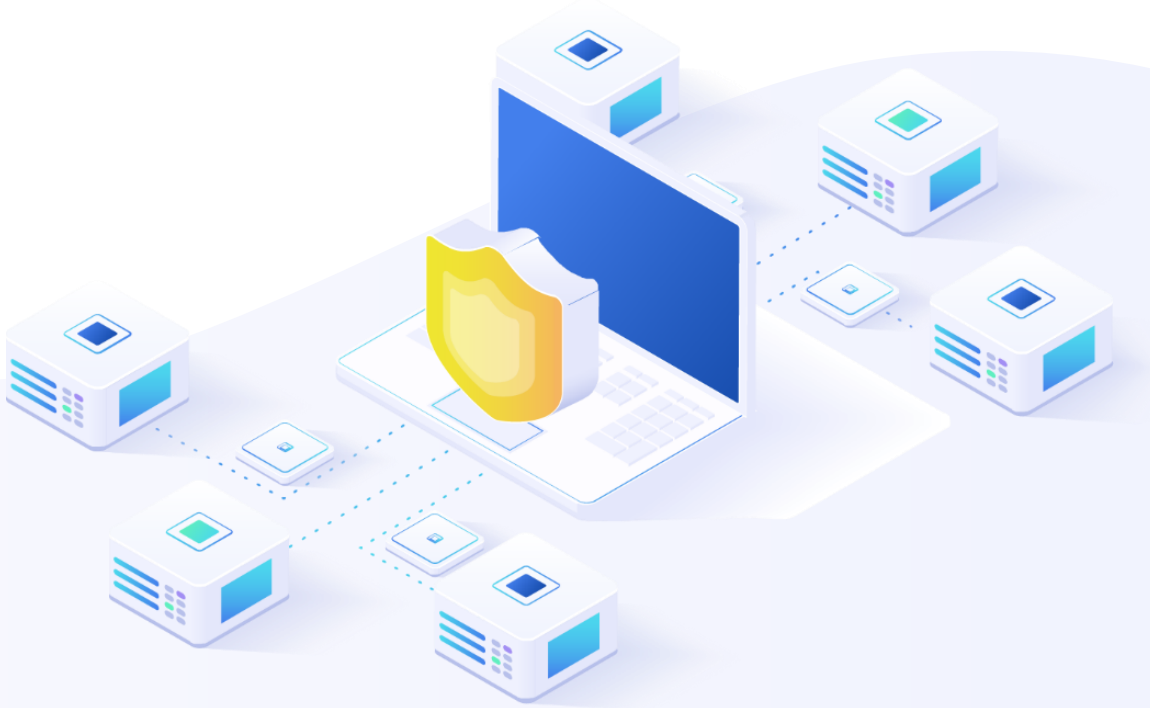
Презентация Компании Юстас

Искусство ИБ

Сертифицированный поставщик решений информационной безопасности



О компании. Цифры и факты

Компания «Юстас» предоставляет широкий спектр услуг по развитию ИТ-инфраструктуры, обеспечению информационной безопасности и экспертной эксплуатации: проектирование, внедрение, модернизация, сопровождение и аудит бизнес-процессов.

13 лет

опыт работы на рынке информационной безопасности и информационных технологий

150+ тех. специалистов

3/4 из них – сертифицированные инженеры различных специализаций

Лицензиат ФСТЭК и ФСБ (слайд 4)

полный комплект лицензий на проведение работ и оказание услуг в области информационной безопасности

50+ партнёров-вендоров

производителей оборудования и ПО

Работаем во всех регионах РФ

Физическое присутствие по всех федеральных округах

500+ реализованных проектов

Из них более 100 проектов федерального масштаба

Техническая и Сервисная поддержка во всех регионах России!

География присутствия и реализованных проектов

Создана сеть для реализации федеральных и региональных проектов с круглосуточной технической поддержкой во всех регионах России

Лицензии компании

1. Лицензия ФСБ России на виды работ, предусмотренных пунктами 12, 13, 20, 21, 22, 25, 28 Положения, утвержденного постановлением Правительства Российской Федерации от 16 апреля 2012г. №313
2. Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации
3. Сертификат соответствия системы менеджмента качества требования ГОСТ Р ИСО 9001-2015 (ISO 9001:2015)
4. Сертификат соответствия системы энергетического менеджмента организации требованиям ГОСТ Р ИСО 50001-2012 (ISO 50001:2018)
5. Сертификат соответствия системы менеджмента информационной безопасности требованиям ГОСТ Р ИСО/МЭК 27001-2013 (ISO 27001:2013)
6. Сертификат соответствия системы менеджмента услуг в сфере информационных технологий требованиям ГОСТ Р ИСО/МЭК 20000-1-2013 (ISO/IEC 20000-1:2011)

Лицензия ФСБ России

Лицензия ФСТЭК России

Сертификат
ISO 9001:2015

Сертификат
ISO 50001:2018

Сертификат
ISO 27001:2013

Сертификат
ISO 20000:2011

Наши партнёры

Yustas

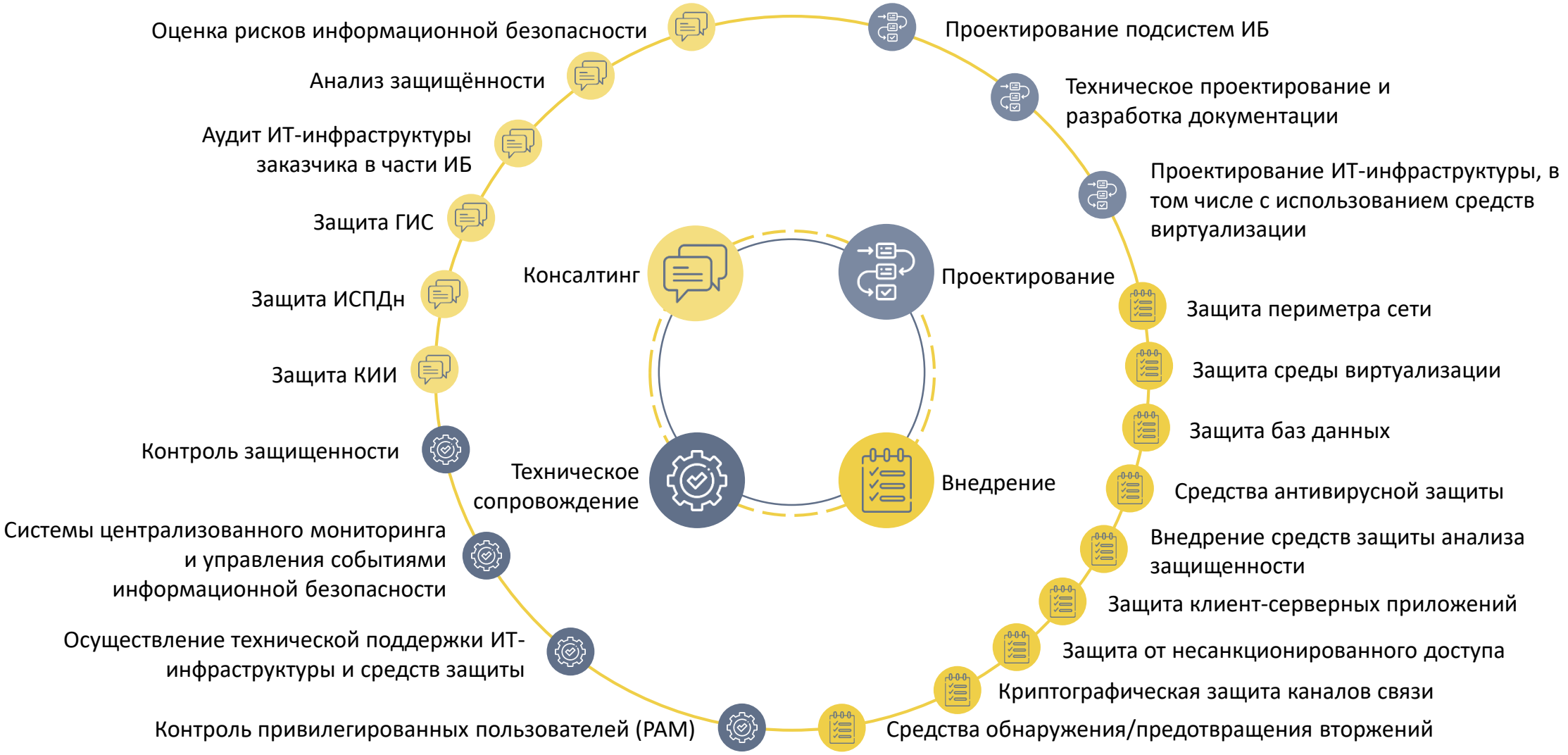
Отечественные производители

КОД БЕЗОПАСНОСТИ
infotecs
kaspersky
positive technologies
SecretTechnologies
SMART-SOFT
s•terra
КРИПТОПРО
base alt
АПР ОКБ
R-Vision
Webinar
Ростелеком Солар
Эшелон комплексная безопасность
Р7-ОФИС
EVERYTAG
РусБИТех-Астра
Avanpost
SECURITY VISION увидеть безопасность
DeviceLock
Аладдин
eltex
ideco
UserGate
ГАРДА ТЕХНОЛОГИИ
АЙТИБАСТИОН
КОНФИДЕНТ инженерные системы

Зарубежные производители

CISCO
JUNIPER NETWORKS
Extreme Connect Beyond the Network
FORTINET
VEEAM
vmware
Acronis
Check Point SOFTWARE TECHNOLOGIES LTD.

Основные направления и услуги



1. Внедрение средств защиты информации /1

1. **Внедрение средств защиты клиент-серверных приложений**

   Оказание услуг по внедрению программных межсетевых экранов, предназначенных для защиты клиент-серверных приложений.

2. **Внедрение средств защиты периметра сети**

   Комплексный подход по ограничению сетевого доступа к защищенным сегментам ИТ-инфраструктуры с использованием средств межсетевого экранирования, средств обнаружения вторжений и VPN-шлюзов.

3. **Внедрение средств защиты от несанкционированного доступа**

   Оказание услуг по внедрению специализированных средств защиты, позволяющих обеспечить защиту, конфиденциальность информации на всех компонентах ИТ-инфраструктуры:

   - Локальные автоматизированные рабочие места пользователей
   - Удаленные рабочие места
   - Файловые сервера и СУБД
   - Почтовые сервера
   - Виртуальная инфраструктура
   - Локальный доступ к оборудованию заказчика

4. **Внедрение средств защиты среды виртуализации**

   Для защиты среды виртуализации используется подход, включающий в себя:

   - Защиту от вредоносного кода
   - Регистрацию действий пользователей
   - Регистрацию действий систем и сервисов
   - Организацию доступности системы с использованием средств резервирования и репликации данных

5. **Внедрение средств криптографической защиты каналов связи**

   - Организации защищенного соединения при использовании конференцсвязи, IP-телефонии и пр.
   - При передаче данных через электронную почту
   - При организации удаленного соединения

1. Внедрение средств защиты информации /2

6. Обеспечение защиты баз данных

Для защиты баз данных от несанкционированного доступа и контроля действий с данными используются специализированные системы, позволяющие:

- Реализовать контроль действий пользователей баз данных
- Осуществлять управление доступом
- Анализ защищенности баз данных
- Централизованное управление системой

7. Внедрение средств обнаружения/предотвращения вторжений

Для выявления фактов неавторизованного доступа в ИТ-инфраструктуру осуществляется внедрение и настройка средств обнаружения/предотвращения вторжений.

8. Внедрение средств антивирусной защиты

Для обеспечения безопасности ИТ-инфраструктуры от вредоносного кода используются средства антивирусной защиты. Специалисты ООО «Юстас» имеют большой опыт во внедрении средств антивирусной защиты на рабочие места пользователей, серверную инфраструктуру, сред виртуализации, внедрение средств Антиспам с централизованным управлением, а также с использованием стратегии эшелонированной защиты.

9. Внедрение средств анализа защищенности

Средства анализа защищенности позволяют в режиме реального времени контролировать состояние защищенности инфраструктуры Заказчика и обеспечить оперативное реагирование на инциденты.

Средства анализа защищенности позволяют:

- Осуществлять централизованный мониторинг состояния уровня защищенности
- Обеспечивать контроль соответствия нормативным техническим требованиям и требованиям заказчика
- Обеспечивать инвентаризацию и контроль изменений информационных ресурсов
- Сокращать затраты на аудит и контроль защищенности

2. Соответствие требованиям

Компания «Юстас» оказывает комплекс услуг для выполнения стандартов и норм при обеспечении информационной безопасности компаний, а также проектированию и разработке проектной и эксплуатационной документации в части ИБ.


Проведение комплексного аудита ИБ


Разработка рекомендаций и документов


Внедрение процессов ИБ


Внедрение средств защиты

Выполнение работ в проектах на соответствие требованиям законодательства, стандартов и лучших практик по ИБ:

- Проектирование с учетом законодательства РФ и нормативных документов (149-ФЗ, 152-ФЗ и связанные правовые акты, приказы ФСТЭК России, приказы ФСБ России, ГОСТ 34, ГОСТ 19 и ГОСТ 2)
- Проектирование систем для компаний разной географической распределённости
- Применение комплексного подхода с учетом отрасли, бизнес-процессов и обрабатываемой информации в компании
- Разработка и актуализация существующей проектной и рабочей документации

При разработке документации учитывается отрасль заказчика, его бизнес-процессы, обрабатываемая информация, применяемые меры защиты. Документация разрабатывается с учетом законодательства РФ и нормативных документов.

3. Консалтинг ИБ

Компания «Юстас» предлагает все виды консалтинговых работ по ИБ, в том числе:

Экспертный аудит ИБ:

- Обследование бизнес-процессов
- Всестороннее обследование ИТ-инфраструктуры
- Анализ процессов ИБ на соответствие лучшим практикам
- Анализ настроек средств защиты информации

Контроль (анализ) защищенности:

- Инвентаризация аппаратного и программного обеспечения
- Сбор конфигурационных файлов систем, служб и СУБД
- Проверка наличия актуальных обновлений компонентов инфраструктуры
- Выявление уязвимостей
- Выявление ошибок конфигурации
- Оценка уровня защищенности ИТ-инфраструктуры

- Анализ рисков ИБ
- Разработка стратегии развития ИБ
- Оценка необходимых ресурсов (кадровых/финансовых/временных) на реализацию мер ИБ
- Выстраивание процессов ИБ в соответствие с выбранной заказчиком методологией

4. Управление доступом. IDM

Портфель решений компании «Юстас» в области комплексного управления правами доступа пользователей включает в себя:

Управление идентификационными данными

- Повышение эффективности процесса управления и контроля прав доступа в ИС
- Снижение нагрузки на подразделение ИТ и ИБ
- Снижение времени ожидания получения прав доступа, а также прохождения аутентификации в ИС
- Снижение рисков нарушения ИБ, связанных с процессом управления правами доступа и аутентификацией

! Вендоры по IDM: Avanpost inRights INFOWATCH®

5. Услуги по мониторингу и реагированию на инциденты ИБ

Преимущества:

- Быстрое развёртывание и масштабирование
- Гибкая модель ценообразования
- Работа с SIEM и СЗИ всех основных производителей

С чем сталкиваются наши клиенты:

- Инциденты ИБ своевременно не выявляются
- Удаётся выполнить реагирование только на малую часть от общего числа инцидентов
- Расследование инцидентов ИБ занимает очень много времени
- Нет возможности получить оперативную информацию о состоянии ИБ в компании

Результаты проекта:

- Выявление инцидентов ИБ, анализ и ликвидация последствий в соответствии с лучшими практиками и требованиями законодательства
- Обработка инцидентов ИБ с учётом оперативного получения актуальных данных об уязвимостях и кибератаках от сторонних центров мониторинга (в т.ч. НКЦКИ, ФинЦерт)
- Передача информации об инцидентах ИБ в НКЦКИ и/или ФинЦерт в рамках выполнения требований 187-ФЗ (672-П)

6. Защита web-приложений

Предлагаемая компанией «Юстас» реализация системы защиты web-приложений позволяет:

- Повысить защищённость и доступность критически важных web-приложений, используемых клиентами и партнёрами
- Контролировать защищённость приложений на всех этапах жизненного цикла, начиная с разработки кода
- Проактивно находить и закрывать уязвимости web-приложений, которыми могут воспользоваться злоумышленники для нанесения ущерба организации
- Оперативно запускать новые интернет-проекты для информирования о продуктах и услугах

Основными компонентами системы непрерывной безопасности web-приложений являются:

- Web Application Scanner (WAS)
- Web Application Firewall (WAF)
- Anti-DDoS

7. Защита от утечек данных и контроль коммуникаций. DLP

Решения для защиты от утечек данных и обеспечения контроля коммуникаций сотрудников позволяют:

- Снизить количество возможных инсайдерских действий, направленных на хищение ценной информации
- Повысить эффективность деятельности за счёт сокращения возможностей для нецелевого использования сотрудниками интернет-ресурсов
- Хранить все данные и проводить анализ инцидентов для дальнейшей подготовки доказательств для разбирательства
- Контролировать качественное исполнение установленных в компании бизнес-процессов

Рекомендации для эффективного использования системы:

- Анализ бизнес-процессов
- Сбор данных и подготовка политик
- Тонкий тюнинг DLP-системы
- Анализ режимов защиты
- Анализ каналов утечек
- Выстраивание режима КТ
- Разработка ОРД
- Обучение работников по вопросам ИБ

8. ИБ АСУ ТП /1

Категорирование объектов критической информационной инфраструктуры

Основания для проведения категорирования:

- Новые требования законодательства, их правильная трактовка и риски неисполнения
- Отсутствие методологии выявления критических процессов и систем, являющихся объектами КИИ
- Сложность организации работ по категорированию и распределения ответственности между подразделениями, ответственными за ИБ, ИТ, сопровождение АСУ ТП, промышленную безопасность, финансовую деятельность и пр.
- Необходимость обосновать руководству какие выгоды помимо «compliance» будут по результатам выполнения работ

Этапы категорирования:

1. Обследование

- Выявление критических процессов (КП)
- Выявление систем автоматизации КП (объектов КИИ)
- Анализ рисков ИБ для систем автоматизации КП и их последствий

2. Разработка/адаптация методологии

- Определение применимых показателей значимости
- Определение и согласование алгоритма расчета показателей
- Разработка рабочих материалов для проведения категорирования

3. Категорирование объектов КИИ

- Организация работы комиссии
- Разработка документации по результатам категорирования
- Разработка перечня и сведений для направления регулятору

4. Планирование мероприятий ИБ

- Определение архитектуры системы безопасности
- Рекомендации по проведению в соответствие требованиям ИБ
- План мероприятий по реализации требований ИБ

8. ИБ АСУ ТП /2

Результаты проекта:

- Консолидированный ответ об обследовании процессов заказчика и состоянии ИБ инфраструктуры за короткий срок
- Формализованный перечень критических процессов и объектов КИИ заказчика
- Методологические материалы, необходимы для организации и выполнения категорирования комиссией (формы расчета показателей значимости, формы протоколов совещаний, положения о деятельности комиссии и пр.)
- Все необходимые в соответствии с законодательством ОРД, содержащие результаты категорирования

- Выполнение требований законодательства и повышение культуры информационной безопасности в компании
- Минимизация рисков финансовых потерь вследствие реализации атаки злоумышленников
- Комплект документации, подтверждающих выполнение требований по информационной безопасности

9. Предоставление комплексной технической поддержки

Специалисты ООО «Юстас» имеют большой опыт и прошли обучение в области IT и ИБ, позволяющее оказывать качественные услуги по сопровождению и эксплуатации.

Многоуровневая система организации технической поддержки в соответствии с лучшими мировыми практиками

Техническая поддержка:

- Корпоративных сетей передачи данных
- Автоматизированных рабочих мест пользователей
- Инфраструктурных сервисов
- Вычислительных ресурсов
- Серверов баз данных и серверов приложений
- Подсистем информационной безопасности

В рамках предоставления услуг специалисты ООО «Юстас» выполняют работы:

- Регламентное обслуживание оборудования
- Контроль действий пользователей и администраторов
- Реагирование на ошибки в работе, восстановление работоспособности
- Контроль и реализация обновлений компонентов
- Мониторинг журналов регистрации событий

Реализованные проекты

Госсектор

РОСРЕЕСТР

Ростелеком

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

ПФР

Ген. прокуратура

ЕГИССО

АНАЛИТИЧЕСКИЙ ЦЕНТР ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТЭК

ГАЗПРОМ

СЕТЬ АЗС ГАЗПРОМНЕФТЬ

РОСНЕФТЬ

Пром-ть, ВПК

НОРНИКЕЛЬ

Ford

RENAULT

MITSUBISHI

Фин. сектор

ГАЗПРОМБАНК

Ренессанс КРЕДИТ

Промсвязьбанк

ВТБ

Альфа Банк

Банк России

Телеком

TELE2

МегаФон

NAUKA оператор цифровых решений

ТОП заказчиков /1

Эксплуатация инфраструктуры единой биометрической системы в АО «Газпромбанк»

ГАЗПРОМБАНК

Техническая поддержка программно-аппаратного комплекса по работе с единой биометрической системой, обеспечивающей выполнение полного набора функций по реализации процессов регистрации биометрических образцов физических лиц в части взаимодействия с ЕСИА и ЕБС, с учетом требований по информационной безопасности.

Подсистема обеспечения информационной безопасности

6 ИБ-комплексов для защиты ИТ-инфраструктуры:

- Комплекс межсетевого экранирования
- Комплекс обнаружения атак
- Комплекс защиты каналов связи
- Комплекс антивирусной защиты
- Комплекс защиты от НСД
- Комплекс анализа защищенности

Задействованы решения 6-ти производителей:

- Лаборатория Касперского
- Код Безопасности
- ИнфоТекс
- КриптоПро
- РусБИТех-Астра
- Доктор Веб
- НПО Эшелон

! Поддержка системы в дневное и ночное время

! Отработка ≈ 300 инцидентов в месяц с соблюдением SLA

ТОП заказчиков /2

Подсистема обеспечения информационной безопасности единой государственной информационной системы социального обеспечения

ЕГИССО

Проектирование и внедрение комплекса программно-технических средств по обеспечению безопасности информации, обрабатываемой в ЕГИССО.

ПОИБ ЕГИССО

Внедрено 9 ИБ-комплексов для защиты ИТ-инфраструктуры:

- Комплекс межсетевого экранирования
- Комплекс обнаружения вторжений
- Комплекс криптографической защиты каналов связи
- Комплекс антивирусной защиты
- Комплекс аутентификации и защиты от НСД
- Комплекс анализа защищённости
- Комплекс защиты веб-приложений
- Комплекс защиты виртуализации
- Комплекс мониторинга действий администраторов

Задействованы решения 5-ти производителей:

- Лаборатория Касперского
- Код Безопасности
- Fortinet
- Positive Technologies
- АйТи БАСТИОН

ТОП заказчиков /3

Защита периметра корпоративной сети и конечных рабочих станций для ПАО «Промсвязьбанк»

Промсвязьбанк

Обеспечение защиты субъектов кии в соответствии с 187-ФЗ.

Внедрено 3 подсистемы ИБ для решения задач:

- Защита каналов связи
- Межсетевое экранирование
- Средство обнаружения вторжений
- Защита от НСД для серверов и рабочих станций

Реализация мер защиты с помощью продуктов «кода безопасности»:

- АПКШ «Континент» с функционалом – КШ/КК/СОВ
- SecretNet Studio

Факты:

- Защищено более 300 субъектов КИИ
- Модернизирована сетевая инфраструктура филиалов
- Развернуто более 10 000 СЗИ от НСД
- Организованно подключение к ГосСОПКА

! «Нарушение стабильной и бесперебойной работы систем критической информационной инфраструктуры (КИИ) не только создает угрозу здоровью и жизни людей, но и негативно влияет на экономическую, политическую и социальную устойчивость региона и государства в целом».

ТОП заказчиков /4

Внедрение системы защиты веб-приложений класса WAF для ПАО «Промсвязьбанк»

Промсвязьбанк

Повышение уровня защищенности информационных ресурсов заказчика путем выявления и реагирования на инциденты информационной безопасности, связанные с эксплуатацией уязвимостей веб-приложений.

Задачи:

- Защита от DDoS-атак
- Обнаружение CSRF / XSS / SQL Injection
- Защита от атак нулевого дня
- Защита веб-приложений от атак OWASP Top 10

Реализация мер защиты с помощью PT Application Firewall:

Факты:

- Обеспечена защита веб-приложений
- Минимизирован риск утечки информации
- Заказчик получил дополнительный инструмент мониторинга информационной безопасности

! «WAF является полезным инструментом в контексте построения эшелонированной защиты веб-приложений».

ТОП заказчиков /5

Защита каналов связи между ЦОД для ПАО «ГМК Норильский никель»

Внедрение СКЗИ на базе высокопроизводительных криптокоммутаторов, задействование всех современных сетевых технологий для достижения доступности и максимальных скоростных показателей с учётом высоких проектных стандартов ПАО «ГМК Норильский никель».

Предъявляемые требования к проектному решению:

- ГОСТ шифрование
- Высокопроизводительное оборудование с минимальным уровнем задержки
- Высокая доступность и минимальное время восстановления при сбое

Реализация:

- Разработка уникального решения с учётом строгих внутренних нормативных требований
- Proof of concept
- Достижение максимальных скоростных показателей для оборудования класса криптокоммутаторов на базе АПКШ «Континент» и S-Terra

Факты:

- 12 ЦОД
- Уникальное решение на базе оборудования АПКШ «Континент» и S-Terra
- Интеграция в существующую сетевую инфраструктуру и смежными системами
- Обучение персонала

! Удалось успешно защитить концепцию и разработать нетиповое решение класса ЦОД.

ТОП заказчиков /6

Внедрение комплекса систем на базе оборудования Fortinet для Аналитического центра при Правительстве Российской Федерации

АНАЛИТИЧЕСКИЙ ЦЕНТР ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Создание настоящей экосистемы, которая позволяет эффективно управлять всеми компонентами системы, а также обеспечивать расширенный мониторинг.

Перечень компонентов системы:

- Компонент межсетевого экранирования FortiGate
- Компонент защиты почтового трафика FortiMail
- Компонент централизованного сбора системных событий и построения отчетов FortiAnalyzer
- Компонент защиты от атак нулевого дня FortisSandbox
- Компонент централизованной аутентификации и авторизации FortiAuthenticator
- Компонент централизованного управления FortiManager

! Проект полностью реализован на продуктах от компании Fortinet.

ТОП заказчиков /7

Мэрия Москвы и органы исполнительной власти

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

Сопровождение миграции информационных систем Департамента Информационных Технологий Москвы в целевой ЦОД, всего более 5000 виртуальных машин, более 200 информационных систем.

Главное управление по информационной безопасности Московской области (ГУРБ МО)

Сопровождение миграции информационных систем Департамента Информационных Технологий Москвы в целевой ЦОД, всего более 5000 виртуальных машин, более 200 информационных систем.

Пенсионный фонд России

Внедрение технологии VDI (виртуальных рабочих столов) в инфраструктуре клиента для 27000 сотрудников заказчика на территории РФ, а также создание и круглосуточная техническая поддержка серверной составляющей комплекса.

Более 70 000 виртуальных рабочих мест.

МЧС Российской Федерации

Установка, настройка новых на замену устаревших программно-аппаратных комплексов шифрования каналов передачи данных и почтовых сообщений в корпоративной сети заказчика в 83+ столицах регионов России в течение 10 недель, всего более 200 устройств.

Более 180 кластеров криптошлюзов, 88 регионов России.

Техническая поддержка

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

ПФР

TELE2

ЭЛЕКТРОННАЯ МОСКВА

МЧС РОССИИ EMERCOM

Ростелеком

Промсвязьбанк

Ген. прокуратура

Ростелеком Солар

Базируемся в Москве, работаем по всей стране

8 (495) 215-02-82

info@ysts.ru

127006, г. Москва, ул. Вятская 27, стр. 15

ИНН: 7707422962

КПП: 770701001

ОГРН: 1187746950555