МТЕ

МультиТек Инжиниринг

ТЕХНОЛОГИЧЕСКАЯ КОМПАНИЯ
В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОНСАЛТИНГ
АУДИТ
ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ
ПОСТАВКА И ВНЕДРЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

www.mte-cyber.by

О компании

Мы создали компанию «МультиТек Инжиниринг» для того, чтобы профессионально оказывать услуги в области информационной безопасности.

Мы уверены, что взрывное развитие информационных технологий будет способствовать росту спроса на услуги по защите данных и обеспечению доступности ИТ-сервисов.

«МультиТек» в переводе с английского означает «множество технологий». Этим мы хотели сказать о том, что для создания эффективной системы защиты необходимо иметь компетенции в большом спектре технологий и продуктов, уметь делать правильный выбор и оптимально интегрировать их.

Мы внимательно следим за мировыми трендами в области кибербезопасности, выводим на рынок и предлагаем заказчикам все самое эффективное, современное, перспективное, обеспечивающее защиту их инвестиций.

На базе передовых технологий и продуктов мы, применяя собственную методологию, разрабатываем решения, которые становятся компонентами проектируемых, создаваемых, внедряемых и сопровождаемых нами систем защиты.

В кадровый состав каждого направления оказываемых нами услуг входят специалисты, сертифицированные производителями используемых компанией продуктов по информационной безопасности. Наряду с непрерывным обучением сотрудников, это позволяет нам поддерживать высокий уровень качества решений и создаваемых на их основе систем.

Наша забота об инвестициях заказчиков проявляется и в том, как уважительно и внимательно мы относимся и тщательно вписываем в создаваемую систему защиты уже имеющиеся в информационном ландшафте средства обеспечения безопасности.

Делая ставку на технологии и продукты, прошедшие апробацию и имеющие положительные отзывы, мы принимаем во внимание и такие характеристики, как простота установки и настройки, качество поддержки продукта производителем (стоимость, условия, время реакции на запросы и др.), перспективы развития продукта.

Мы понимаем и не скрываем от наших заказчиков, что любая защита преодолевается. Именно поэтому мы проектируем и создаем системы, в которых сбалансированы технологии прогнозирования, предотвращения атак, детектирования, реагирования на инциденты информационной безопасности с технологиями и средствами восстановления бизнес-сервисов после успешной атаки.

Мы стремимся обеспечить киберустойчивость бизнеса наших заказчиков, но понимаем, что это своеобразный идеал, дорога к которому лежит через внедрение оптимальных процессов системы менеджмента информационной безопасности, инвентаризацию активов, управление рисками, выбор и оркестрацию эффективных технологий безопасности.

Качество нашей работы гарантируется сертификатами менеджмента качества СТБ ISO 9001-2015 и менеджмента информационной безопасности СТБ ISO/IEC 27001-2016 применительно к проектированию, созданию, аттестации и сопровождению систем защиты информации информационных систем и систем управления технологическими процессами.

Услуги

Руководствуясь системным подходом к информационной безопасности (ИБ), мы предлагаем комплекс консалтинговых услуг, включающий следующие этапы:

тестирование на проникновение

аудит информационной безопасности (включая КВОИ)

разработка концепции (стратегии) развития системы обеспечения ИБ

проектирование системы защиты информации (включая КВОИ)

внедрение программных и/или технических средств защиты информации (с обеспечением 1-й линии технической поддержки)

аттестация системы защиты информации

сопровождение системы обеспечения ИБ

Тестирование на проникновение проводится с целью выявления существующих уязвимых мест в элементах ИТ-инфраструктуры, демонстрации возможности использования уязвимостей (на примере наиболее критических) и формирования рекомендаций по устранению выявленных уязвимостей.

Аудит систем информационной безопасности (включая системы информационной безопасности критически важных объектов информатизации - КВОИ) проводится в соответствии с требованиями действующего законодательства. В результате аудита дается объективная оценка состояния системы информационной безопасности с рекомендациями по устранению выявленных недостатков, составляется дорожная карта мероприятий по совершенствованию системы информационной безопасности.

Полученная по результатам аудита оценка может использоваться при формировании концепции (стратегии) развития системы обеспечения ИБ, а также при формализации и внедрении процессов обеспечения ИБ.

Последнее предполагает разработку политики безопасности и целого ряда других локальных нормативных документов, определяющих требования по защите информации и порядок их выполнения. Внедрение процессов может осуществляться с учетом международных и отечественных стандартов по защите информации.

При проектировании систем защиты информации осуществляется выбор конкретных решений, которые будут использоваться для защиты информационных ресурсов. При необходимости производятся стендовые испытания решений.

Далее выполняются работы по установке и настройке средств защиты, входящих в состав решений системы защиты информации, разрабатывается эксплуатационная документация, проводится обучение персонала.

На заключительных этапах проводится аттестация системы защиты и оказываются услуги по техническому сопровождению системы защиты информации.

Мы предоставляем описанные выше услуги как в комплексе, так и по отдельности, в зависимости от задач, стоящих перед заказчиком.

Такой подход позволяет поэтапно выполнять работы по реализации комплекса организационно-технических мер защиты, давая заказчику возможность эффективно распределить по времени необходимые инвестиции.

Решения для инфраструктурной безопасности

Мы поставляем, настраиваем и сопровождаем следующие типы решений для защиты ИТ-инфраструктуры и ее компонентов.

Защищаемый компонент ИТ-инфраструктуры	Тип решения
ИТ-инфраструктура	Управление сетевой безопасностью (Firewall Management)
	Защита баз данных (DataBase Security)
	Межсетевые экраны (Firewalls)
	Обнаружение/предотвращение вторжений (Intrusion Detection System – IDS, Intrusion Prevention System – IPS)
	Системы противодействия целевым атакам (Advanced Persistent Threat) – Anti-APT
	Системы мониторинга трафика
	Системы класса Deception
	Защита каналов связи
	Защита виртуальных сред
	Средства перенаправления web-трафика (Web-proxy)
	Защита от спама
	Защита от 0-Day атак
	Система сканирования уязвимостей
	Системы резервного копирования и восстановления информации
Конечные точки	Антивирусная защита (Anti-Virus Protection - AVP)
	Системы обнаружения атак и реагирования на них (Endpoint, Detect & Response - EDR)
	Защита банкоматов
	Контроль подключения внешних устройств
Доступ	Системы управления корпоративной мобильностью (Enterprise Mobile Management - EMM)
	Идентификация и контроль доступа к сети (Network Access Control - NAC)
	Системы управления многофакторной (расширенной) аутентификацией (Multi-Factor Authentication – MFA или Advanced Authentication – AA)
Web	Защита web-приложений и сайтов (Web Application Firewall - WAF)
	Защита от DDoS атак

Решения, учитывающие влияние на ИБ поведения людей (People-Centric Security)

При создании систем обеспечения ИБ мы придерживаемся принципиальной позиции - ИБ не должна ограничивать развитие бизнеса. Вместо запретов и ограничений, исполнение которых порой сложно контролировать, мы предлагаем заказчикам создавать и развивать культуру ИБ, поощряющую правильную (безопасную) работу с информацией, информационными системами и сервисами (так называемая концепция человекоцентричной безопасности, People-Centric Security, PCS). Мы убеждены, что следование концепции PCS повышает личную ответственность сотрудников, снижает количество их ошибок и позволяет все это контролировать в прозрачном режиме.

Для реализации концепции PCS мы предлагаем следующие решения.

Название системы	Класс	Функции
Автоматизированная система управления учетными записями и правами пользователей (создается на базе продуктов класса Identity Management)	IDM	Автоматизирует управление учетными записями и правами пользователей в информационных системах заказчика, построения ролевых моделей, аудита имеющихся доступов
Автоматизированная система контроля за действиями привилегированных пользователей (создается на базе продуктов класса Privileged Account Management)	PAM	Обеспечивает контроль за действиями системных администраторов, специалистов подрядчиков, аудиторов и других пользователей с расширенными правами
Автоматизированная система защиты от утечек конфиденциальной информации (создается на базе продуктов класса Data Loss Prevention)	DLP	В режиме реального времени анализирует все информационные потоки для контроля переписки по электронной почте, голосовых и текстовых сообщений, переданных файлов, информации, отправляемой на облачные сервисы или принимаемой с них, внешних устройств, документов, отправляемых на печать и т.д. и сообщает о возможных инцидентах
Автоматизированная система противодействия мошенничеству (создается на базе продуктов класса Anti-fraud)	AFR	Автоматизирует контроли для борьбы с: • внутренним мошенничеством; • клиентским и/или платежным мошенничеством в системах дистанционного банковского обслуживания; • неплатежным мошенничеством (закупки, склад, учет и т. д.)
Автоматизированная система тестирования и обучения сотрудников практической кибербезопасности	APH	Имитирует фишинговые атаки, выявляет сотрудников с недостаточным уровнем знаний и/или навыков в области ИБ и предоставляет инструменты для обучения
Автоматизированный анализатор исходного кода приложений	SAST	Позволяет анализировать код приложений на наличие уязвимостей

Решения для центров управления ИБ

В связи с ростом количества и масштабов компьютерных атак, а также в соответствии с требованиями законодательства в области ИБ, растут потребности в комплексных решениях, направленных на предотвращение инцидентов, оценку состояния и управления рисками ИБ.

Для успешного оперативного реагирования на инциденты ИБ необходимо осуществлять сбор и анализ событий ИБ, проводить оценку влияния выявленного инцидента на критичные бизнес-процессы, вести системную работу по локализации, реагированию, расследованию и ликвидации последствий инцидентов ИБ, вырабатывать меры по исключению повторения инцидентов ИБ и улучшению защитных мер. В организациях с разветвленной территориально-распределенной структурой эффективным средством снижения материальных затрат и потребности в квалифицированных кадрах является централизация средств контроля и управления ИБ. Все эти задачи призван решать **центр управления ИБ.**

Для центров управления ИБ мы предоставляем следующие решения.

Название системы	Класс	Функции
Автоматизированная система мониторинга, корреляции и анализа событий ИБ (создается на базе решений класса Security Information and Event Management	SIEM	Обеспечивает получение информации о событиях ИБ из различных источников (межсетевые экраны, средства защиты баз данных и приложений, средства контроля за работой пользователей, операционные системы и др.) анализирует их, в результате чего определяет и сигнализирует о появлении инцидентов
Автоматизированная система мониторинга и управления инцидентами ИБ (создается на базе решений класса Incident Response Platform)	IRP	Обеспечивает инвентаризацию ИТ-активов, регистрировать инциденты ИБ, назначать и контролировать задачи по работе с инцидентами, запускать преднастроенные алгоритмы и автоматизированные сценарии, которые обеспечивают быстроту реакции и слаженность действий команды реагирования, помогая свести к минимуму возможные негативные последствия от инцидента
Автоматизированная система управления данными кибер-разведки (создается на базе решений класса Threat Intelligence Platform – TIP)	TIP	Обеспечивает автоматический сбор, нормализацию и обогащение индикаторов компрометации, передачу обработанных данных напрямую на внутренние средства защиты, а также поиск и обнаружение индикаторов во внутренней инфраструктуре заказчика с помощью сенсоров
Автоматизированная система управления информационной безопасностью (создается на базе решений класса Security Governance, Risk, Compliance	SGRC	Обеспечивает автоматизацию таких процессов, как: • управление рисками ИБ; • моделирование угроз; • аудит, оценка соответствия требованиям ИБ; • контроль и управление ИТ-активами; • планирование и контроль задач специалистов по ИБ, управление рабочими процессами

Решения для защиты информации в АСУ ТП

Мы активно развиваем направление информационной безопасности АСУ ТП.

Компания обладает практическим опытом аудита ИБ АСУ ТП, проектирования систем защиты информации АСУ ТП (включая КВОИ).

Для АСУ ТП некоторых отраслей промышленности разработаны и апробированы типовые решения по защите информации.

Компания является партнером крупнейших производителей средств защиты информации АСУ ТП и сотрудничает со всеми известными производителями АСУ ТП.

Проектирование и создание системы защиты информации АСУ ТП мы ведем с учетом таких факторов, как:

- специфичные особенности каждой АСУ ТП;
- отсутствие отлаженных процедур взаимодействия служб сопровождения АСУ ТП с корпоративными ИТ-, ИБ-службами;
- применение в АСУ ТП проприетарных протоколов;
- ограничения по применению стандартных средств защиты информации;
- невозможность остановки технологических процессов;
- неактуальность имеющейся документации.

Компания предлагает услуги по проектированию и созданию как отдельных подсистем, так и комплексной системы защиты информации АСУ ТП.

При выборе средств защиты мы практикуем проведение пилотных проектов, в ходе которых заказчик убеждается в эффективности предлагаемого решения и отсутствии негативного влияния на функционирование АСУ ТП.

Система защиты АСУ ТП, как правило, включает следующие подсистемы.

Подсистемы
Защиты от несанкционированного доступа
Безопасного межсетевого взаимодействия
Анализа защищенности
Антивирусной защиты
Мониторинга событий ИБ
Физической защиты

При проектировании системы защиты информации АСУ ТП и внедрении средств защиты мы уделяем большое внимание ее интеграции в комплексную систему обеспечения ИБ предприятия, обучению персонала, а также проведению киберучений персонала АСУ ТП с целью практической отработки внештатных ситуаций.

Наши партнеры

R-Vision
At the root of your security
Стратегический партнер

POSITIVE TECHNOLOGIES

kaspersky

GROUP-IB

Jet

INDEED ID

Ростелеком
Солар

Acronis

Антифишинг

MICRO FOCUS

UserGate

TEKVEL

LibraSoft

CYBERARK

Check Point
SOFTWARE TECHNOLOGIES LTD.

imperva

RAPID7

FUDO
SECURITY

TREND MICRO

SOC PRIME
POWER ON SECURITY

WALLIX
CYBERSECURITY SIMPLIFIED

veeAM

МультиТек Инжиниринг

Республика Беларусь, 220030,
г. Минск, ул. Революционная, 24Б - 28

info@mte-cyber.by

+375 17 28 28 959

www.mte-cyber.by