



**МультиТек Инжиниринг**

киберустойчивость заказчиков – наша миссия





# СОДЕРЖАНИЕ

О КОМПАНИИ .....	3
ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ .....	5
СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ .....	6
РЕШЕНИЯ (КЛАССЫ РЕШЕНИЙ) ДЛЯ АВТОМАТИЗАЦИИ ЗАДАЧ И ПРОЦЕССОВ .....	7
АТТЕСТАЦИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ .....	9
ТЕХНИЧЕСКАЯ ПОДДЕРЖКА .....	10
ЛИЦЕНЗИИ И СЕРТИФИКАТЫ .....	11
ПАРТНЕРЫ .....	12



## О КОМПАНИИ

Белорусская компания **«МультиТек Инжиниринг»** (Общество с ограниченной ответственностью «МультиТек Инжиниринг») с 2019 года работает над тем, чтобы сделать организации и предприятия киберустойчивыми – способными противодействовать кибератакам и, при необходимости, восстанавливать свою деятельность в приемлемые сроки.

«МультиТек Инжиниринг» – это инженерная команда профессионалов-единомышленников в области кибербезопасности.

Наши заказчики работают в сферах государственного управления, финансов, машиностроения, энергетики, нефтехимии, пищевой промышленности, торговли, образования, здравоохранения и др.

Мы постоянно ищем, тестируем и выводим на рынок новые продукты (решения, услуги), в эффективность которых сами искренне верим.

На основе предлагаемых продуктов мы создаем и внедряем системы защиты информации, включая разработку документации, обучение персонала эксплуатации, ввод в эксплуатацию и техническую поддержку.

Мы начинаем любой проект с формирования видения – описания того, как будет выглядеть и функционировать система, которую мы задумали. Для нас более важен контент, который мы порождаем, чем технологии, которые используются для этого.

Мы оформляем наш опыт в методики, которые становятся корпоративными стандартами и базой знаний, используются и совершенствуются нашими сотрудниками в ходе практической деятельности.

**Если требования заказчика вынуждают отступить от наших ценностей, мы не боимся сказать «нет» и объяснить свою позицию. Мы порекомендуем обратиться к конкуренту, который, возможно, предложит требуемое заказчиком решение.**

**Мы не боимся того, что конкуренты скопируют наши продукты, потому что мы сами являемся частью этих продуктов, распространяя свой образ мышления на маркетинг, продажу, проектирование, создание, техническую поддержку систем.**

**Мы учимся у многих, но никогда и никого не копируем, поскольку имитатор не может лидировать, а всегда догоняет.**

Мы не говорим: «Специалистов нет», мы делаем все возможное, чтобы они были: инвестируем в образование детей в области безопасности, в подготовку студентов и курсантов – будущих специалистов по киберзащите, обучаем персонал эксплуатации в ходе внедрения систем.

Мы постоянно расширяем свои компетенции и готовы к решению любых задач по обеспечению кибербезопасности.



# ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Мы проектируем систему защиты информации (далее – СЗИ) информационной системы (далее – ИС) заказчика в тесном контакте с его ИТ- и ИБ-специалистами. Ведь спроектировать эффективную СЗИ – это наша общая задача, и на время проектирования мы – единая команда.

Особенно важен первый этап проектирования – аудит (обследование) текущего состояния защищенности (для владельцев КВОИ аудит должен проводиться не реже 1 раза в год) на предмет соответствия действующему законодательству по защите информации. Мы смотрим на СЗИ «со стороны», как профессионалы, чтобы оценить ее эффективность и, при необходимости, разработать рекомендации по ее повышению.

Мы с большим уважением относимся к труду ИТ- и ИБ-специалистов заказчика, поэтому в ходе проектирования стремимся максимально учесть и сохранить все, что наработано заказчиком. Наша задача – обеспечить кибербезопасность с минимально необходимыми ограничениями для бизнес-процессов и пользователей ИС.

Мы помогаем заказчику сформировать видение будущей СЗИ, спроектировать систему управления кибербезопасностью, аккуратно вписать ее в действующую систему менеджмента. При необходимости консультируем по вопросам категорирования информации и разработки акта отнесения ИС к типовым классам информационных систем.

Вместе с заказчиком мы формируем перечень необходимых средств защиты информации (далее – СрЗИ) с указанием их рыночной стоимости, разрабатываем стратегию создания СЗИ с учетом возможностей заказчика по инвестированию.

В ходе проектирования мы разрабатываем проекты локальных правовых актов, регламентирующих основные процессы ИБ. Этим мы облегчаем заказчику решение задачи создания СЗИ, в ходе которой он должен внедрить и автоматизировать эти процессы.

Мы всегда защищаем проект СЗИ перед высшим руководством заказчика, поскольку без участия первого лица трудно ожидать выделения необходимых инвестиций и выполнения организационных мероприятий по созданию СЗИ. В ходе общения мы обращаем внимание на необходимость вовлечения всех пользователей ИС в обеспечение кибербезопасности, объясняем необходимость регулярного обучения, проведения киберучений, постоянной и системной работы по совершенствованию СЗИ.



# СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Создаваемые нами системы защиты информации (далее – СЗИ) включают различные компоненты, обеспечивающие в совокупности эшелонированную защиту информационной системы заказчика.

Каждый компонент, как правило, представляет собой систему, базирующуюся на определенном программном обеспечении (далее – решение).

Для того, чтобы заказчик мог осознанно выбрать требуемое решение, мы проводим пилотные проекты. Цель пилотного проекта – на базе решения создать прототип системы, выполняющей соответствующую задачу по защите информации заказчика.

В ходе пилотного проекта мы обучаем персонал заказчика самостоятельной работе по настройке решения, администрированию и эксплуатации прототипа системы. При этом большое внимание уделяем разработке документации, позволяющей далее развить прототип до полномасштабной системы.

Создаваемые нами системы проходят стадии разработки технического задания и технического проекта (разрабатываются документы «Пояснительная записка», «Программа и методика испытаний»), приемо-сдаточных испытаний и ввода в эксплуатацию.

Мы делаем все необходимое, чтобы заказчик мог самостоятельно эксплуатировать систему. На этапе ввода системы в эксплуатацию разрабатывается эксплуатационная документация (содержит описание параметров, на которые настроена система, способов интеграции системы с другими СЗИ, приемов и способов эксплуатации системы в конкретных условиях применения). На площадке заказчика проводится обучение персонала эксплуатации системы по согласованной программе.

Руководствуясь этим подходом, мы успешно реализовали в Республике Беларусь и странах СНГ проекты создания интегрированных систем защиты информации на основе решений классов SIEM (сбор и мониторинг событий информационной безопасности), IRP/SOAR (автоматизация реагирования на инциденты информационной безопасности), SGRC (автоматизация управления активами, оценки рисков и аудитов), PAM (контроль за работой привилегированных пользователей) и др., накопив значительный практический опыт.

ПРОЦЕССЫ И ЗАДАЧИ ИБ		РЕШЕНИЯ (КЛАССЫ РЕШЕНИЙ) ДЛЯ АВТОМАТИЗАЦИИ ЗАДАЧ И ПРОЦЕССОВ ИБ		ПРОИЗВОДИТЕЛЬ РЕШЕНИЯ	
Защита конечных точек	AVPO EDR			АО «Лаборатория Касперского»	
Защита инфраструктуры	NTA МЭ			АО «Позитив Технолоджиз» ООО «Юзергейт» ООО «Код Безопасности»	АО «Лаборатория Касперского» Check Point Software Technologies Ltd ООО «Нетхаб»
Инвентаризация активов	ACP			ООО «Р-Вижн»	
Управление уязвимостями	IRP/SOAR Mp8 VM			ООО «Р-Вижн» АО «Позитив Технолоджиз» АО «Позитив Технолоджиз»	
Управление рисками ИБ	SGRC			ООО «Р-Вижн»	
Контроль соответствия стандартам и аудиты	SGRC Mp8			ООО «Р-Вижн» АО «Позитив Технолоджиз»	
Защита веб-приложений и сайтов	WAF			АО «Позитив Технолоджиз»	
Управление доступом пользователей	IAM PAM			ООО «Индид»	
Защита от утечек информации	DLP			АО «ИнфоВотч»	
Киберразведка	TI TIP			АО «Лаборатория Касперского» ООО «Р-Вижн»	
Приманки и ловушки	honeypot и deception			ООО «Р-Вижн»	
Управление жизненным циклом инцидента	SIEM IRP/SOAR			АО «Позитив Технолоджиз» АО «Лаборатория Касперского» ООО «Р-Вижн»	
Обучение пользователей	ASAP Антифишинг			АО «Лаборатория Касперского» ООО «Антифишинг»	
Защита информации в БД и файлах	DCAP/DAG DAM			ООО «Сайберпик» ООО «Гарда Технологии»	
Анализатор исходного кода	SAST, DAST			АО «Позитив Технолоджиз» ООО «Солар Секьюрити»	
Защита от DDoS-атак	Периметр			ООО «Гарда Технологии»	
Защита каналов связи	BelVPN			ООО «С-Терра Бел»	
Защита от спама	KSMG			АО «Лаборатория Касперского»	
Защищенная виртуализация	Брест			ООО «РусБИТех-Астра»	
Резервное копирование и восстановление	RuBackup			ООО «РУБЭКАП»	
Защита АСУ ТП	ISIM KICS			АО «Позитив Технолоджиз» АО «Лаборатория Касперского»	



# АТТЕСТАЦИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Выполняя работы по аттестации системы защиты информации (далее – СЗИ) информационной системы заказчика, мы делаем все, чтобы убедиться в качестве созданной СЗИ.

Мы разрабатываем и согласовываем с заказчиком программу и методику испытаний.

В ходе аттестации наши эксперты внимательно анализируют документацию на СЗИ, эффективность применяемых организационных и технических мер защиты информации.

Анализу также подвергается система управления информационной безопасностью, наличие и уровень подготовки персонала эксплуатации средств защиты информации, готовность заказчика эффективно реагировать на инциденты кибербезопасности, корректировать СЗИ по результатам анализа инцидентов и целый ряд других вопросов.

Кроме этого, проводятся необходимые технические испытания и проверки.

Мы делаем это беспристрастно, но с огромным уважением к той работе, которую провел заказчик в ходе проектирования и создания СЗИ.

При обнаружении недостатков, не позволяющих аттестовать СЗИ, мы тщательно разрабатываем перечень рекомендаций, обсуждаем с заказчиком способы и порядок устранения проблем.

Мы делаем все от нас зависящее, чтобы аттестованная СЗИ результативно защищала, а не просто находилась на балансе заказчика.

Аттестацией СЗИ не заканчивается наше взаимодействие с заказчиком. Мы и дальше готовы работать с ним по любым вопросам обеспечения киберустойчивости.



## ТЕХНИЧЕСКАЯ ПОДДЕРЖКА СОЗДАВАЕМЫХ СИСТЕМ

Мы обеспечиваем техническую поддержку системы, созданной на базе продвигаемых компанией решений (далее – программное обеспечение, ПО), с даты подписания акта сдачи-приемки системы.

Поскольку мы уполномочены производителями оказывать услуги 1-й линии гарантийного обслуживания ПО в рамках технической поддержки системы, то рекомендуем заказчикам по всем вопросам, касающимся эксплуатации ПО и системы, обращаться в наш контакт-центр.

### ТЕХНИЧЕСКАЯ ПОДДЕРЖКА СИСТЕМЫ ОСУЩЕСТВЛЯЕТСЯ НАМИ ПО СЛЕДУЮЩЕМУ АЛГОРИТМУ:

- На стадии приемки обращения (заявки) мы делаем все, чтобы получить четкую постановку задачи (при необходимости – с выездом к заказчику).
- Систематизируем собранную информацию, анализируем проблему, находим решение задачи (при необходимости выезжаем к заказчику для реализации решения).
- При невозможности устранить проблему своими силами обращаемся в службу технической поддержки производителя ПО и передаем все собранные сведения, а также указываем приемлемые для заказчика сроки устранения проблемы.
- Контролируем сроки устранения проблемы.
- В случае, если решить проблему в приемлемые сроки не представляется возможным, предлагаем заказчику временное решение.
- Перед передачей заказчику способа устранения проблемы тестируем предлагаемое решение на собственном стенде.
- На этом же стенде тестируются все обновления ПО, полученные от производителя, перед передачей их заказчику.
- Периодически заказчику направляются сообщения, информирующие об обновлениях и новых возможностях ПО, оптимальных способах и приемах эксплуатации.
- Вне зависимости от возникающих проблем, регулярно (не реже 1 раза в квартал) мы общаемся со службой эксплуатации заказчика для получения информации об удовлетворенности ПО и качеством технической поддержки системы, а также пожеланий по совершенствованию ПО и технической поддержки. Информация обрабатывается, систематизируется и направляется производителю ПО.



# ЛИЦЕНЗИИ И СЕРТИФИКАТЫ

Лицензия Оперативно-аналитического центра при Президенте Республики Беларусь на право осуществления деятельности по технической и (или) криптографической защите информации (включая КВОИ)



Сертификат соответствия системы менеджмента качества требованиям СТБ ISO 9001-2015, ISO 9001:2015



Сертификат соответствия системы менеджмента информационной безопасности требованиям СТБ ISO/IEC 27001-2016, ISO/IEC 27001-2013



## НАМ ДОВЕРЯЮТ

- Национальный банк Республики Беларусь
- ОАО «Сберегательный банк «Беларусбанк»
- ЗАО «МТБанк»
- ОАО «Белорусская универсальная товарная биржа»
- РУП «Минскэнерго»
- РУП «Могилевэнерго»
- РУП «Витебскэнерго»
- Филиал «ПСДТУ» РУП «Гродноэнерго»
- ОАО «Западэлектросетьстрой»
- ГУ «Госэнергогазнадзор»
- СЗАО «Безопасные дороги Беларуси»
- ОАО «Минский завод колесных тягачей»
- ОАО «Кузлитмаш»

- ОАО «Белшина»
- ОАО «Химремонт»
- ОАО «Минск Кристалл»
- ОАО «Борисовский завод медицинских препаратов»
- ГУО «Белорусская медицинская академия последипломного образования»
- Белорусский государственный медицинский университет
- Белорусский государственный университет информатики и радиоэлектроники
- РНПЦ медицинской экспертизы и реабилитации
- СООО «ТрайплФарм»
- M.F.GE (Грузия)



## ПАРТНЕРЫ

**R-Vision**

Стратегический партнер

 positive  
technologies

 kaspersky



КОМПАНИЯ  
ИНДИД

  
ГАРДА  
ТЕХНОЛОГИИ

 Ростелеком  
Солар

 UserGate

  
**CHECK POINT**

 Антифишинг

  
INFOWATCH

 s•terra  
B E L

 АСТРА  
группа компаний

**F.A.C.T.**

 АЙТИБАСТИОН

 CYBERPEAK  
системы защиты данных

 CTRLHACK

 Нетхаб®  
сеть под контролем

 КОД  
безопасности



# ДЛЯ ЗАПИСЕЙ





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



+375 17 28-28-959



[info@mte-cyber.by](mailto:info@mte-cyber.by)  
(для документов)

[support@mte-cyber.by](mailto:support@mte-cyber.by)  
(техническая поддержка)



[www.mte-cyber.by](http://www.mte-cyber.by)

