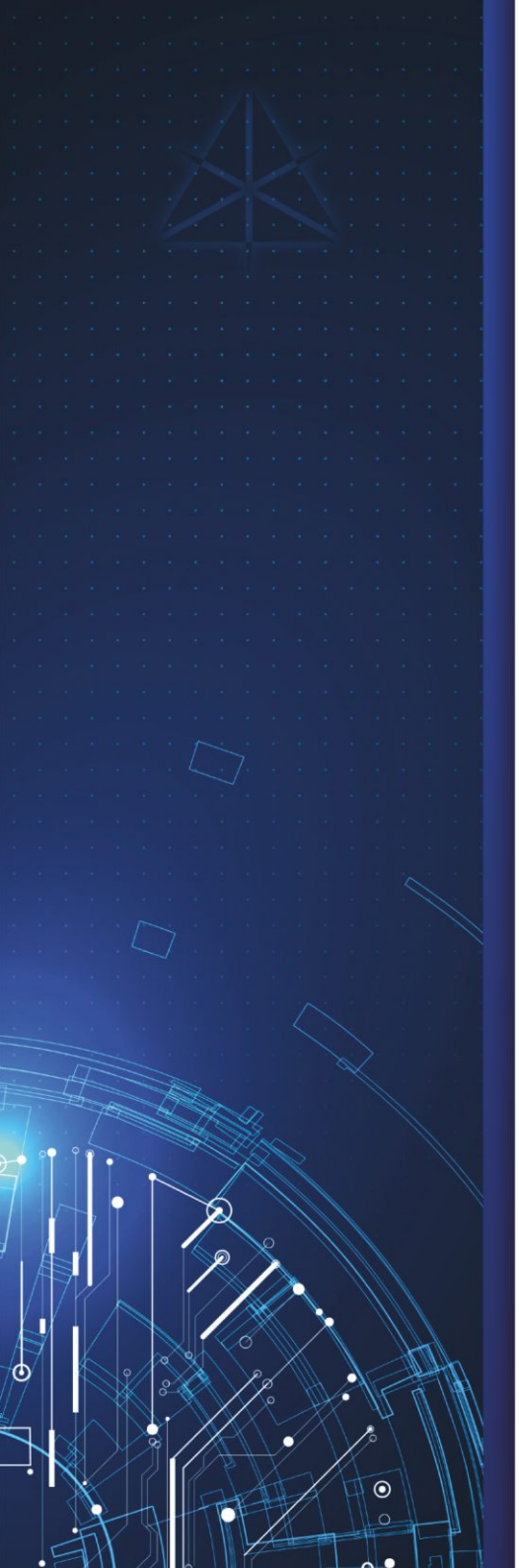

МТЕ

МультиТек Инжиниринг

киберустойчивость заказчиков – наша миссия

СОДЕРЖАНИЕ

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 проектируем и создаем центры кибербезопасности, системы защиты информации, включая разработку документации, обучение персонала эксплуатации 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 нас, потому что сами являемся частью нашего образа мышления, распространяя его на маркетинг, продажу, проектирование, создание и 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 И СОЗДАНИЕ КОРПОРАТИВНЫХ ЦЕНТРОВ КИБЕРБЕЗОПАСНОСТИ

Мы проектируем и создаем корпоративные центры кибербезопасности (далее – ЦК), соответствующие действующему законодательству по защите информации.

Опыт внедрения средств защиты информации, которые являются компонентами ЦК, позволил нам разработать собственную методику создания ЦК, в основе которой лежат две стратегии:

● «ЦКБыстро!»; ● «ЦКплавно».

Реализация стратегии «ЦКБыстро» позволяет за 6 месяцев спроектировать ЦК, развернуть, настроить и интегрировать его компоненты, разработать необходимую эксплуатационную документацию и регламенты, обучить персонал эксплуатации, спроектировать, создать и аттестовать систему защиты информации информационной системы ЦК, подготовить ЦК к аттестации.

Затем аттестованный ЦК переводится в режим функционирования, в ходе которого персонал эксплуатации при нашей консалтинговой поддержке продолжает работы по тщательной отладке процессов, подключению объектов мониторинга, разработке новых правил корреляции, совершенствованию регламентов, повышению квалификации персонала эксплуатации и т.д.

Стратегия «ЦКплавно» предполагает создание ЦК путем постепенного приобретения и внедрения необходимых программных компонентов, отладки их функционирования, интеграции и подготовки персонала эксплуатации. Эта стратегия позволяет распределить во времени необходимые инвестиции, уделить больше внимания отладке каждого компонента, однако увеличивает интервал времени, через который ЦК может перейти в режим полноценного мониторинга кибербезопасности.

Обе стратегии предполагают, что работы по проектированию и созданию ЦК выполняются вместе со специалистами заказчика, входящими в команду эксплуатации ЦК. Для них мы проводим теоретические и практические занятия с обязательным тестированием знаний и навыков.

В рамках технической поддержки ЦК мы обеспечиваем поставку и проведение обновлений программных компонентов ЦК, оказываем консультационную помощь по вопросам его эксплуатации.

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 – наша общая задача, и на время проектирования мы – единая команда.

Особенно важен первый этап проектирования – обследование текущего состояния защищенности на предмет соответствия действующему законодательству по защите информации. Мы смотрим на СЗИ «со стороны», чтобы оценить ее эффективность и, при необходимости, разработать рекомендации по совершенствованию.

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 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	АВПО EDR	АО «Лаборатория Касперского» АО «Лаборатория Касперского» / АО «Позитив Текнолоджиз»
Защита инфраструктуры	NTA, «Песочница»	АО «Лаборатория Касперского» ООО «АВ Софт» / АО «Позитив Текнолоджиз»
Защита периметра	МЭ и управление	ООО «Юзергейт» / ООО «Нетхаб» ООО «Код безопасности» / Check Point Software Technologies Ltd.
Защита трафика (FTP, HTTP(S))	KWTS	АО «Лаборатория Касперского»
Управление уязвимостями	IRP/SOAR MP8 VM	ООО «Р-Вижн» АО «Позитив Текнолоджиз» ООО «Р-Вижн» / АО «Позитив Текнолоджиз»
Управление рисками ИБ	SGRC	ООО «Р-Вижн»
Контроль соответствия стандартам и аудиты	SGRC MP8, VM	ООО «Р-Вижн» АО «Позитив Текнолоджиз» / ООО «Р-Вижн»
Защита веб-приложений и сайтов	WAF	ООО «СолидСофт» / АО «Позитив Текнолоджиз»
Управление доступом пользователей	IAM PAM	ООО «Индид»
Защита от утечек информации	DLP	АО «ИнфоВотч» / ООО «Тэксод Технолоджиз»
Кибербразведка	TIP	ООО «Р-Вижн» / АО «Лаборатория Касперского»
Приманки и ловушки	honeypot и deception	ООО «Р-Вижн»
Управление жизненным циклом инцидента	SIEM IRP/SOAR	АО «Лаборатория Касперского» / АО «Позитив Текнолоджиз» / ООО «РуСИЕМ» 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	DerSecur Ltd. / АО «Позитив Текнолоджиз»
Защита от DDoS-атак	Периметр	ООО «Гарда Технологии»
Защита от спама	KSMG	АО «Лаборатория Касперского»
Защищенная виртуализация	Брест Zstack	ООО «РусБИТех-Астра» Zstack International Information Technologies Limited
Резервное копирование и восстановление	RuBackup Vinchin	ООО «РУБЭКАП» Chengdu Vinchin Technology Co., Ltd.
Защита АСУ ТП	KICS / ISIM Диод данных	АО «Лаборатория Касперского» / АО «Позитив Текнолоджиз» АО «Лаборатория Касперского» / ООО «АйТи Бастион» / АО «АМТ-Груп»

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, анализировать их причины, планировать и проводить мероприятия по предотвращению 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.

ЗАЩИТА ИНФОРМАЦИИ В АСУ ТП

Активно развивая направление информационной безопасности АСУ ТП, мы накопили опыт проектирования и создания систем защиты информации, обрабатываемой в технологических сетях.

Для АСУ ТП целого ряда отраслей промышленности нами разработаны и апробированы типовые решения по защите информации.

В этой работе мы сотрудничаем с известными производителями АСУ ТП и средств защиты информации.

Проектируя и создавая системы защиты информации АСУ ТП, мы учитываем такие факторы, как:

- специфичные особенности каждой АСУ ТП;
- применение в АСУ ТП проприетарных протоколов;
- ограничения по применению стандартных средств защиты информации;
- невозможность остановки технологических процессов

и некоторые другие.

При выборе средств защиты в конкретном проекте мы практикуем пилотирование решений, в ходе которых заказчики убеждаются в их эффективности и отсутствии негативного влияния на функционирование АСУ ТП.

При проектировании и создании системы защиты информации АСУ ТП мы уделяем большое внимание вопросам эффективной интеграции применяемых средств защиты, взаимному обогащению информацией о событиях безопасности, автоматизации обнаружения уязвимостей промышленного оборудования, мониторингу и реагированию на киберинциденты на конечных узлах, возможностям для контроля конфигураций и проведения аудита безопасности.

ПРОЕКТИРОВАНИЕ, СОЗДАНИЕ И АУДИТ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНОГО ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Проектирование и создание систем информационной безопасности (далее – СИБ) объектов, нарушение или прекращение функционирования информационных систем которых может иметь негативные социальные, политические, экономические и экологические последствия (далее - критически важные объекты информатизации, КВОИ), - одно из ключевых направлений нашей деятельности.

В ходе проектирования и создания СИБ мы тесно взаимодействуем с персоналом КВОИ при выполнении таких работ, как:

- определение перечня основных угроз и нарушителей ИБ КВОИ;
- разработка методологии оценки рисков ИБ КВОИ и проведение оценки таких рисков;
- определение требований к параметрам настройки программных, программно-аппаратных средств и средств защиты информации по обеспечению ИБ КВОИ и блокированию (нейтрализации) угроз ИБ КВОИ;
- определение средств, необходимых для реализации плана обработки рисков;
- разработка локальных правовых актов КВОИ.

Мы стремимся к тому, чтобы в результате нашей совместной с заказчиком работы на КВОИ были внедрены эффективные и сбалансированные правовые, организационные, технические меры, направленные на обеспечение ИБ.

Особенно большое внимание мы уделяем вопросам обучения персонала КВОИ, слаженной работе подразделений, задействованных в процессе реагирования на инциденты ИБ.

В ходе выполнения работ по аудиту СИБ КВОИ мы считаем своей задачей помочь заказчику объективно оценить степень защищенности СИБ и вместе с ним разработать действенные меры по ее совершенствованию.

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 извещения, 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 27001-2024, ISO/IEC 27001:2022

НАМ ДОВЕРЯЮТ

- Национальный банк Республики Беларусь
- ОАО «Сберегательный банк «Беларусбанк»
- ОАО «Белагропромбанк»
- ОАО «Банк развития Республики Беларусь»
- ОАО «Банковский процессинговый центр»
- ЗАО «МТБанк»
- РУП «Белтелеком»
- 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 «Белшина»
- ОАО «Светлогорский ЦКК»
- ОАО «Кузлитмаш»
- ОАО «Химремонт»
- ОАО «МИНСК КРИСТАЛЛ» - управляющая компания холдинга «МИНСК КРИСТАЛЛ ГРУПП»
- ОАО «Витебский ликеро-водочный завод «Придвинье»
- ОАО «Борисовский завод медицинских препаратов»
- ГУ «Республиканский научно-практический центр медицинских технологий, информатизации, управления и экономики здравоохранения»
- Белорусский государственный медицинский университет
- ГУ «Республиканский научно-практический центр медицинской экспертизы и реабилитации»
- ГУ «Республиканский научно-практический центр трансфузиологии и медицинских биотехнологий»
- Белорусский государственный университет информатики и радиоэлектроники
- СООО «ТрайплФарм»
- ОАО «Беллакт» Волковыск

ПАРТНЕРЫ

R-Vision
Стратегический партнер

kaspersky

positive technologies

КОМПАНИЯ ИНДИД

ГАРДА

СОЛАР

UserGate

CHECK POINT

КОД безопасности

DS ЦИФРОВЫЕ РЕШЕНИЯ

INFOWATCH

АСТРА

AVANPOST

F.A.C.C.T.

АЙТИБАСТИОН

CYBERPEAK
системы защиты данных

CTRLHACK

Нетхаб
сеть под контролем

Start X

DerSecur

AVSOFT

falcongaze

RUSIEM
Всё под контролем

solidwall

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

+375 17 28-28-959
+375 44 70-28-959
(отдел продаж)

+375 44 72-28-959
(техническая поддержка)

info@mte-cyber.by
(для документов)

support@mte-cyber.by
(техническая поддержка)

MTE

МультиТек Инжиниринг

www.mte-cyber.by