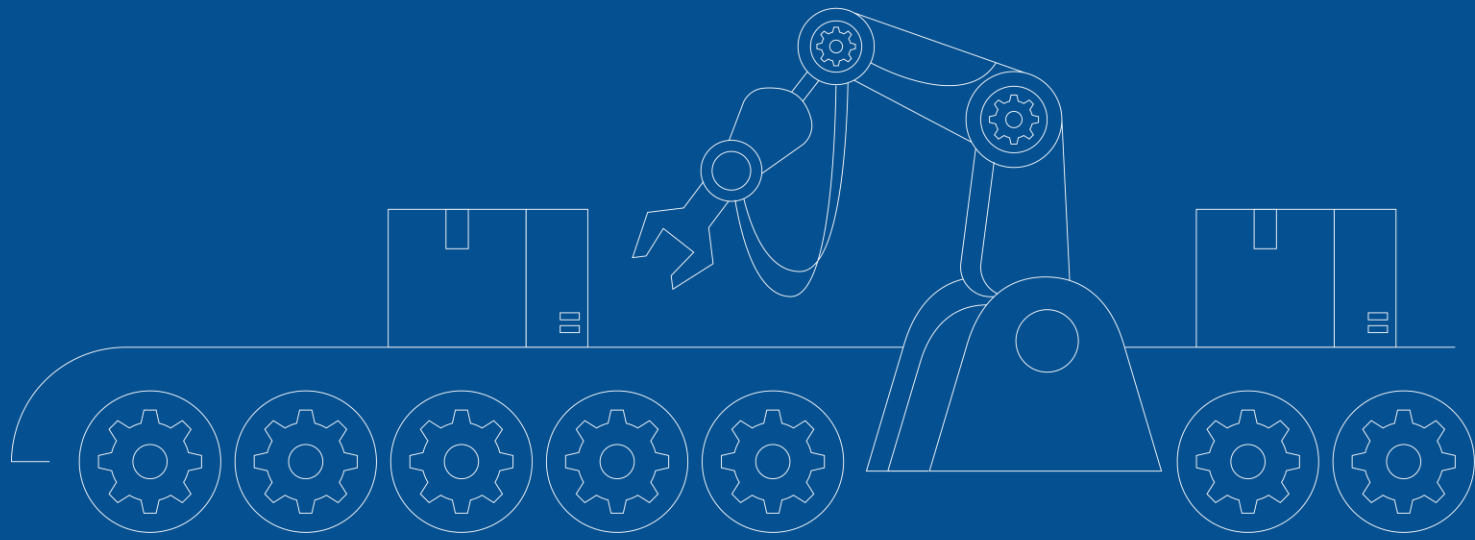
Мы знаем всё о цифровой трансформации!

Ваш надёжный партнёр в информационной безопасности

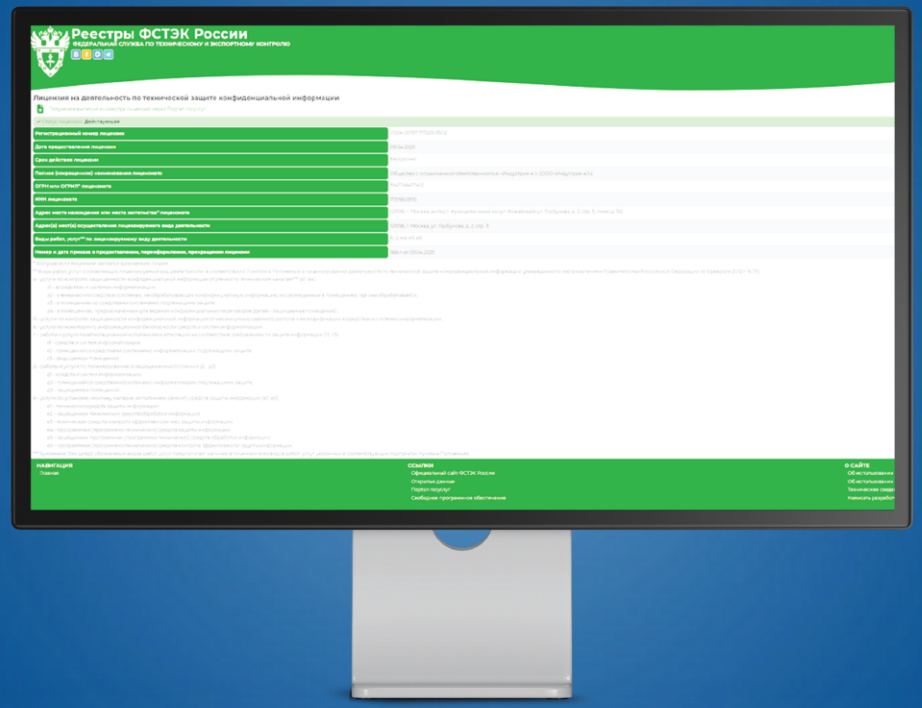


Индустрия 4.1

Наши лицензии и сертификаты

02

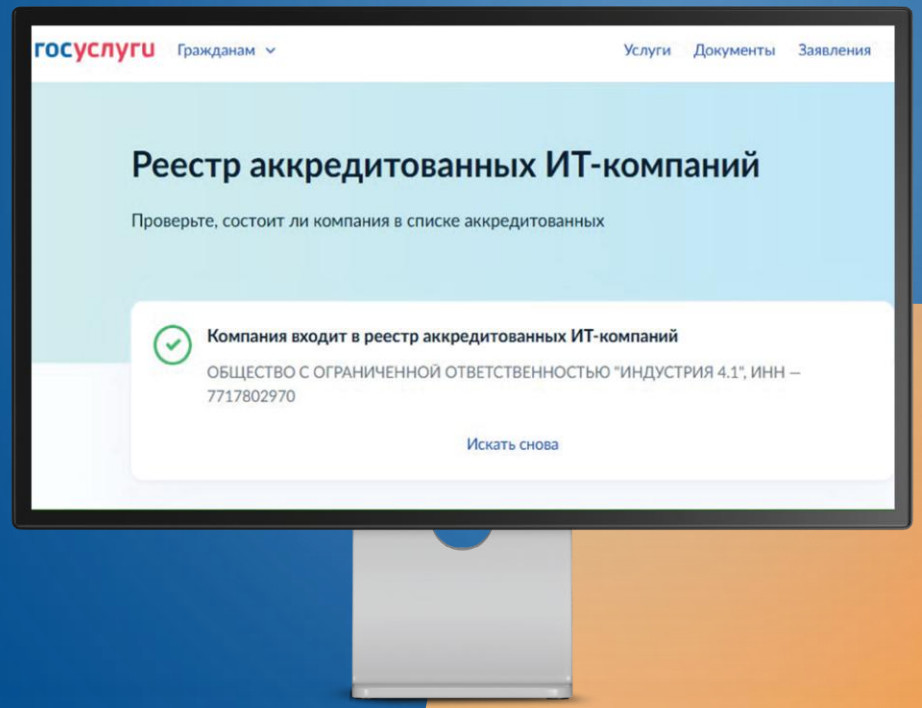
Лицензия ФСТЭК



ООО «Индустрия 4.1» имеет лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации

Регистрационный номер Л024-00107-77/02103502 от 09.04.2025 г.

Аккредитация ИТ-компании



ООО «Индустрия 4.1» включено в реестр аккредитованных ИТ-компаний

Информационная безопасность — это цифровой иммунитет современного предприятия и неотъемлемый элемент его устойчивого функционирования

Наши решения

01 Идентификация и аутентификация

04 Защита машинных носителей информации

07 Обнаружение компьютерных атак

02 Управление доступами

05 Аудиты безопасности

08 Защита АСУ

03 Ограничения программной среды

06 Антивирусная защита

09 Защита технических средств и систем

Идентификация и аутентификация

Основа всей системы защиты информации

Индустрия 4.1

05

Необходимость внедрения

В результате внедрения мер по идентификации и аутентификации снижаются риски утечек информации, обеспечивается соблюдение требований регуляторов, вырастает защищённость критичных активов

Преимущества внедрения

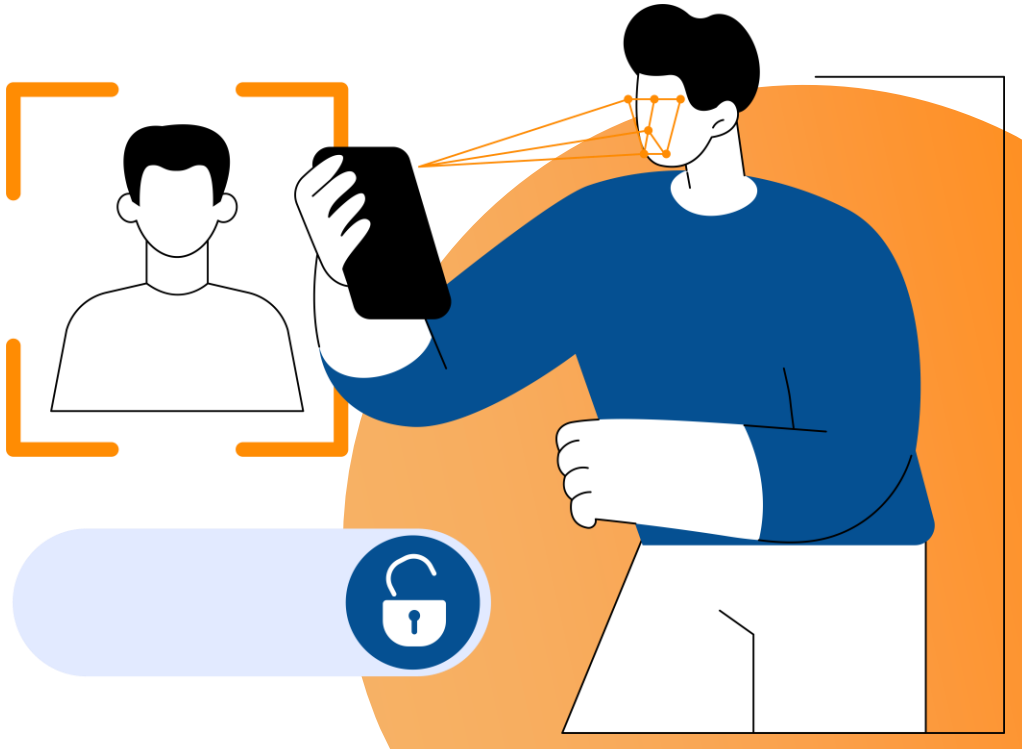
01 Повышение уровня защищённости

02 Персональная ответственность пользователей

03 Защита непрерывности производственных процессов

Функции системы

- Предотвращение несанкционированного доступа
- Обеспечение подотчётности действий пользователя
- Разграничение прав доступа
- Защита конфиденциальности информации
- Соблюдение законодательных и регуляторных требований
- Противодействие угрозам "отказ в обслуживании" (DoS) и сканированию



Управление доступами

Безопасность через контроль доступа

Индустрия 4.1

06

Описание решения

Обеспечение безопасности данных за счёт строгого контроля доступа пользователей к информационным ресурсам и системам. Это позволяет гарантировать, что доступ к данным, системам и функциям предоставляется только авторизованным пользователям в пределах их должностных обязанностей и полномочий.

Преимущества внедрения

01 Снижение рисков утечек, искажения или уничтожения данных предприятия

02 Персональная ответственность пользователя за выполняемые действия

03 Предотвращение несанкционированного доступа к информации и критическим системам

Необходимость внедрения

- Ресурсы требуют защиты от третьих лиц, не имеющих доступа к ним
- Пользователям не нужно предоставлять доступ к большему количеству данных, чем ему требуется для выполнения поставленной задачи
- Необходимы контроль и надзор за тем, какой пользователь к каким данным получает доступ
- Данные должны быть изолированы, но при этом доступны даже при распределённом хранении

Обеспечение ограничений программной среды

Индустрия 4.1

07

Необходимость внедрения

Предотвращает выполнение несанкционированного, вредоносного или потенциально опасного программного кода в системах предприятия, а также снижает риски нарушения информационной безопасности и устойчивости технологических процессов

Преимущества внедрения

01 Предотвращает заражение вредоносным ПО, в том числе через съёмные носители и внешние подключения

02 Обеспечивает стабильную и предсказуемую работу информационных систем и АСУ ТП

03 Минимизирует последствия ошибок пользователей и инсайдерских действий

Функции системы

- Запуск только предварительно одобренных программ, всё неавторизованное ПО блокируется по умолчанию
- Централизованное управление ПО через доверенную систему управления ИТ-активами уполномоченными на это администраторами
- Ограничение исполнения скриптов из не доверенных источников, контроль за запуском PowerShell, Bash, макросов.
- Сегментация и изоляция сред исполнения. Применяются технологии виртуализации и контейнеризации для опасных и специализированных задач
- Обновление разрешённого ПО до актуальных версий

Обеспечение защиты машинных носителей информации

Индустрия 4.1

08

Необходимость внедрения

Предотвращение утраты, компрометации и несанкционированного распространения данных, хранящихся и обрабатываемых на предприятии, снижение рисков информационных и производственных инцидентов

Организационные и технические меры

01 Учёт и инвентаризация обеспечиваются регистрацией всех физических накопителей информации

02 Шифрование данных, обязательное полное шифрование для ноутбуков и съёмных носителей информации

03 Регламентация использования съёмных носителей с техническими ограничениями в критичных случаях

04 Контроль за выносом носителей информации за пределы контролируемой зоны и их утилизацией

05 Защита от аппаратных угроз, реализованных на уровне прошивок устройств

При обеспечении защиты машинных носителей информации снижается риск инцидентов даже при физической утере носителя, обеспечиваются конфиденциальность данных и соответствие регуляторным требованиям.

Внедрение мер по обеспечению защиты машинных носителей информации ***является обязательным элементом комплексной защиты данных и технологических процессов на предприятии***.

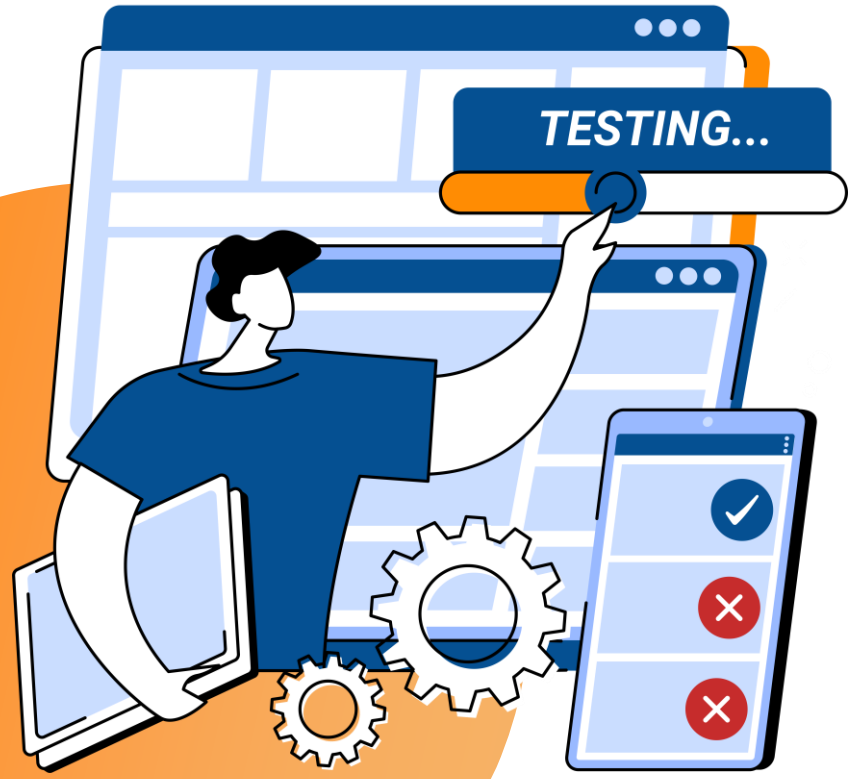
Аудиты безопасности

Оценка эффективности систем защиты

Индустрия 4.1

Необходимость внедрения

Безопасность требует постоянного контроля за своим состоянием и подтверждения соответствия различным требованиям. Назначение аудита – быть инструментом для анализа и улучшения защищённости, выявления слабых мест в защите, повышения уровня безопасности.



01 Планирование аудитов

Аудиты должны быть запланированы и выполняться периодически, либо внепланово при определённых событиях (внедрение новой системы, инцидент)

02 Объекты проверки при аудите

1. Документация
2. Технические средства
3. Процессы

03 Методы проведения аудита

1. Интервью работников
2. Анализ документации
3. Технический скрининг
4. Тесты на проникновение

04 Ключевые этапы аудита

1. Подготовка: определяются границы аудита, цели, состав комиссии
2. Сбор доказательств определёнными методами
3. Формирование отчёта: анализ и оценка рисков, фиксация несоответствий, формирование рекомендаций по устранению выявленных замечаний
4. Исправление и контроль в соответствии с планом корректирующих действий

Антивирусная защита

Обнаружение и нейтрализация вредоносного ПО

Индустрия 4.1

Это базовый элемент системы защиты!

Он должен работать комплексно и непрерывно, адаптируясь к современным угрозам, поскольку с появлением доступного ИИ для создания вредоносного ПО у злоумышленников, полагаться только на сигнатурный анализ становится всё более опасно.

Защите должны подлежать

- Рабочие станции
- Серверы
- Мобильные устройства
- Сетевое оборудование
- Информационный трафик
- Электронная почта

Ключевые принципы организации

01 По возможности, использование единой консоли для мониторинга, настройки и формирования отчётов

02 Регулярное обновление сигнатур с минимальным временным промежутком от выхода новой базы до её обновления в системе антивирусной защиты

03 Обязательная установка и активация средств защиты на всех устройствах, имеющим доступ к защищаемым ресурсам, включая BYOD (личные устройства сотрудников, используемые для работы)

Современные технологии (NGAV)

01 Поведенческий анализ и машинное обучение для обнаружения Zero-day угроз

02 Контроль приложений и устройств, блокировка неавторизованных ПО и носителей

03 Изоляция подозрительных объектов в песочнице для анализа их поведения

Обнаружение и предотвращение компьютерных атак (кибератак)

Индустрия 4.1

IDS (Intrusion Detection System)

система обнаружения атак и аномалий (сигнализирует)

IPS (Intrusion Prevention System)

система предотвращения атак (обнаруживает и блокирует), не применяется для автоматизированных систем

Автоматизированные системы управления технологическими процессами (АСУ ТП)

1. Характеризуются длительным жизненным циклом и использованием устаревших ОС и протоколов
2. Требуют непрерывной и стабильной работы, где любые сбои могут привести к авариям, простоям и ущербу

Этапы внедрения решения на объекте

01 Консультирование

02 Обследование

03 Формирование ТЗ

04 Проектирование

05 Реализация

06 Внедрение

Создание системы «иммунного надзора» сети

- Предотвращает финансовые потери от кибератак
- Защищает ваши репутацию и данные
- Обеспечивает непрерывность бизнес-процессов

Защита технических средств и систем

Повышение устойчивости промышленных ИТ-систем

12

Преимущества внедрения

Обеспечение комплексной физической и логической сохранности ИТ-инфраструктуры, направленное на предотвращение несанкционированного доступа, вывода из строя и компрометации оборудования, а также системного программного обеспечения.

01 **Физическая защита доступа** в серверные, ЦОДы, телекоммуникационные шкафы реализуется множеством технических средств и их комбинированием (электронные пропуска, видеонаблюдение, охрана и т.д.)

02 **Физическая защита инженерных систем** обеспечивает стабильность климата в помещениях размещения ИТ-активов, стабильное электропитание, гарантированное пожаротушение

03 **Безопасная конфигурация** подразумевает под собой не только базовые меры вроде отключения неиспользуемых сервисов, портов, учётных записей по умолчанию, смены заводских паролей, но и регулярное обновление прошивок, ОС, драйверов, в совокупности с защитой загрузочной среды

04 **Безопасность на уровне архитектуры** и её эксплуатации путём логической сегментации и изоляции сетей, применения безопасных сетевых протоколов

Защита технических средств требует комплексного подхода – от физической безопасности до безопасной настройки, это одна из базовых мер в системе обеспечения безопасности.

Эффективность мер зависит от строгости контроля за их исполнением.

Технологический суверенитет и импортозамещение

Импортозамещение

Это не просто ответ на вызовы времени, а **долгосрочная стратегия**, позволяющая сохранить независимость, укрепить экономику и заложить основу для прорывов в эпоху цифровизации.

Мы постоянно совершенствуем свою экспертизу в области отечественных разработок, работаем совместно с российскими производителями и разработчиками, чтобы наши заказчики внедряли программы импортозамещения на современном, не уступающем иностранным аналогам оборудовании.

Технологический суверенитет

Технологический суверенитет идёт дальше, он подразумевает способность **самостоятельно разрабатывать и внедрять инновации** в стратегических областях промышленности.

Для нас технологический суверенитет — это не просто лозунг, а практическая работа. Внедряя российские решения в АСУ ТП и ИТ, мы строим цифровую инфраструктуру, которой можно доверять, которая защищена от внешних угроз и обеспечивает устойчивость критически важных объектов и бизнес-процессов наших заказчиков. Мы видим высокий потенциал отечественных разработок и продолжаем активно расширять их использование в наших проектах.

Наши партнёры

Индустрия 4.1

Оборудование и программное обеспечение

DLP	Системы предотвращения утечки данных
IAM	Системы управления идентификацией и доступом к ресурсам
PAM	Системы контроля привилегированных учётных записей
NGFW	Средства межсетевого экранирования нового поколения
IDS	Системы обнаружения вторжений
IPS	Системы предотвращения вторжений
SIEM	Системы мониторинга событий информационной безопасности
IRS	Системы автоматизации реагирования на инциденты информационной безопасности
NFT	Инструменты для сетевой криминалистики, мониторинга и анализа сетевого трафика

Перечень поставщиков решений в области ИБ

kaspersky
АЛЬТКОРП
INFOWATCH
ORION SOFT
eltex
GIS ГАЗИНФОРМСЕРВИС
SECURITY code
infotecs
pt
UserGate
INFODIODE
КИБЕРПРОТЕКТ
Dr.WEB Сделано в России
ИНДИД
R-Vision
АЙТИБАСТИОН
SOLAR
с•терра

Наши контакты

i41.ru

+7 (495) 108-99-87

info@i41.ru

Цифровая трансформация – это путь, а не проект с чёткими рамками

г. Москва

ул. Горбунова, 2
строение 3, офис 192

Бизнес центр
«Гранд Сетунь Плаза»