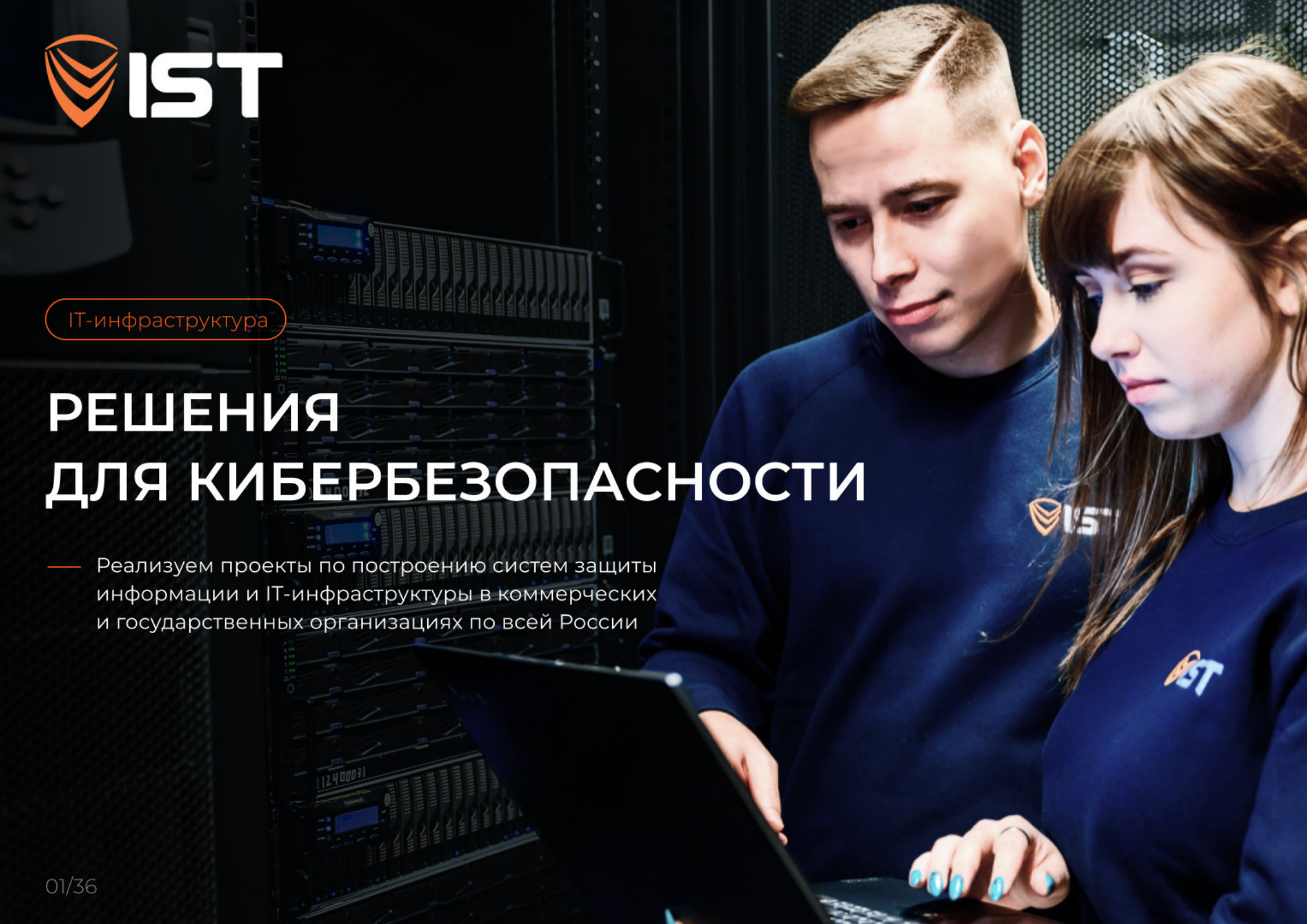
IST

IT-инфраструктура

РЕШЕНИЯ ДЛЯ КИБЕРБЕЗОПАСНОСТИ

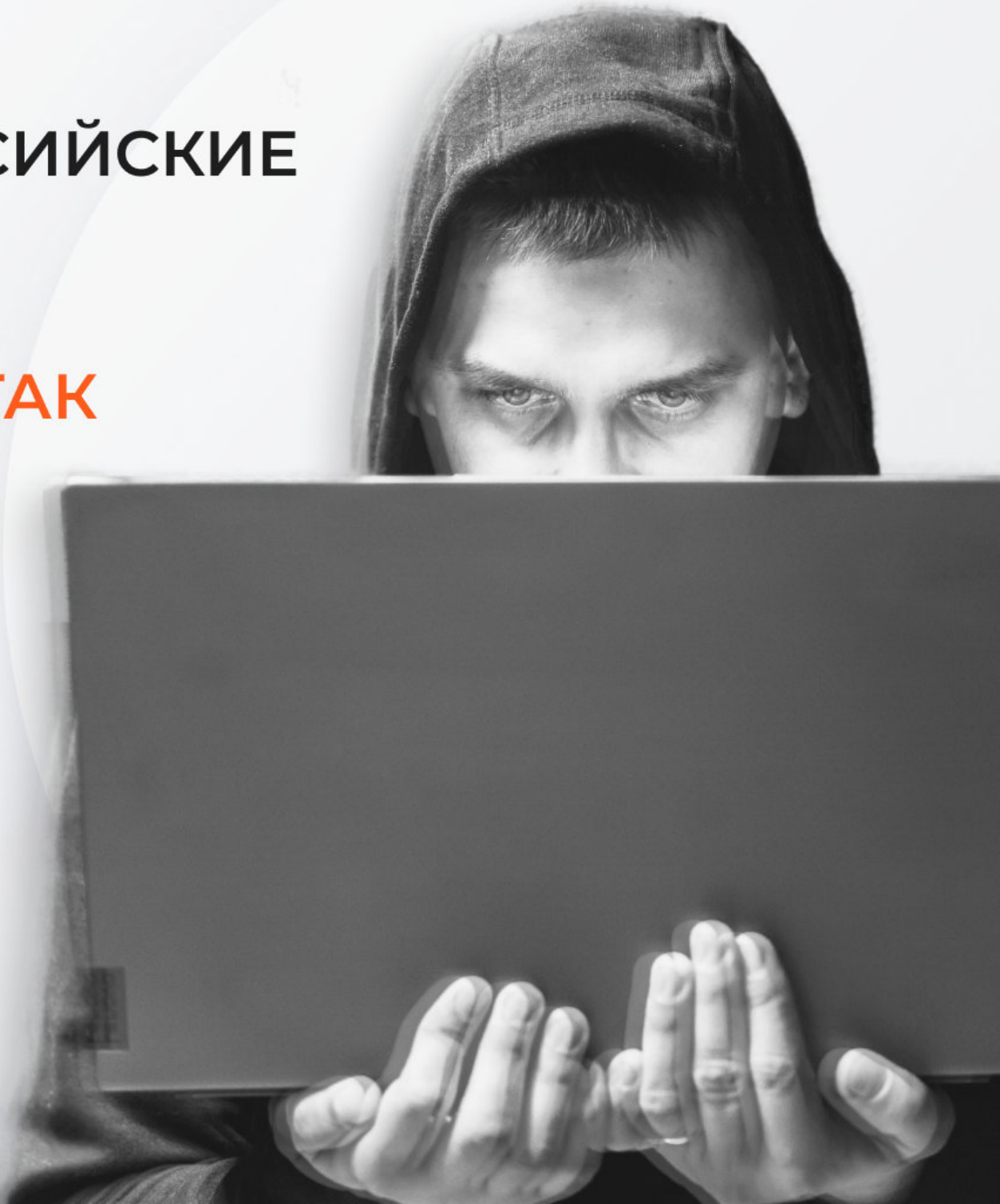
— Реализуем проекты по построению систем защиты информации и IT-инфраструктуры в коммерческих и государственных организациях по всей России



ЗА 2022 ГОД НА РОССИЙСКИЕ КОМПАНИИ БЫЛО СОВЕРШЕНО ОКОЛО 1 МЛН ХАКЕРСКИХ АТАК

Средний ущерб от одной успешной кибератаки составляет для крупного бизнеса **более 50 млн рублей,** для среднего и малого бизнеса **– 2,5 млн. рублей**

Каждое четвертое преступление в России совершается с помощью информационных технологий



*Данные приведены на основании данных «Ростелеком-Солар» от 20 февраля 2023 года

К сожалению, не существует системы информационной безопасности, дающей 100% гарантию защиты от киберугроз

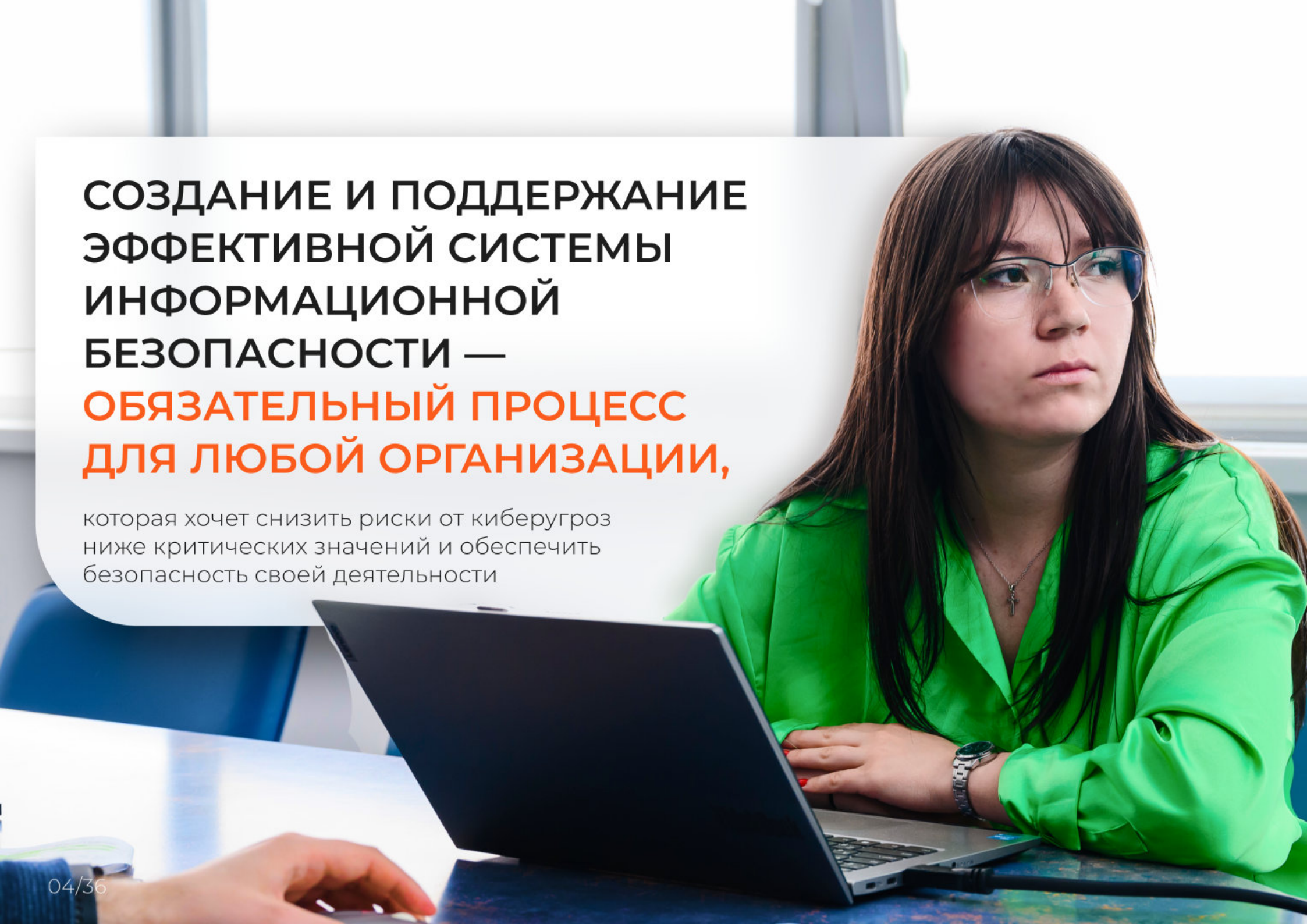
ПРИ ЭТОМ ВОЗМОЖНО ПОСТРОИТЬ СИСТЕМУ ЗАЩИТЫ, КОТОРАЯ БУДЕТ ГАРАНТИРОВАТЬ:

- бесперебойную работу критичных для функционирования организации процессов
- снижение ущерба от инцидентов ИБ ниже максимально допустимых для организации значений

Правильная система ИБ – это совокупность технических средств, людей и процессов

СОЗДАНИЕ И ПОДДЕРЖАНИЕ ЭФФЕКТИВНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ — ОБЯЗАТЕЛЬНЫЙ ПРОЦЕСС ДЛЯ ЛЮБОЙ ОРГАНИЗАЦИИ,

которая хочет снизить риски от киберугроз ниже критических значений и обеспечить безопасность своей деятельности

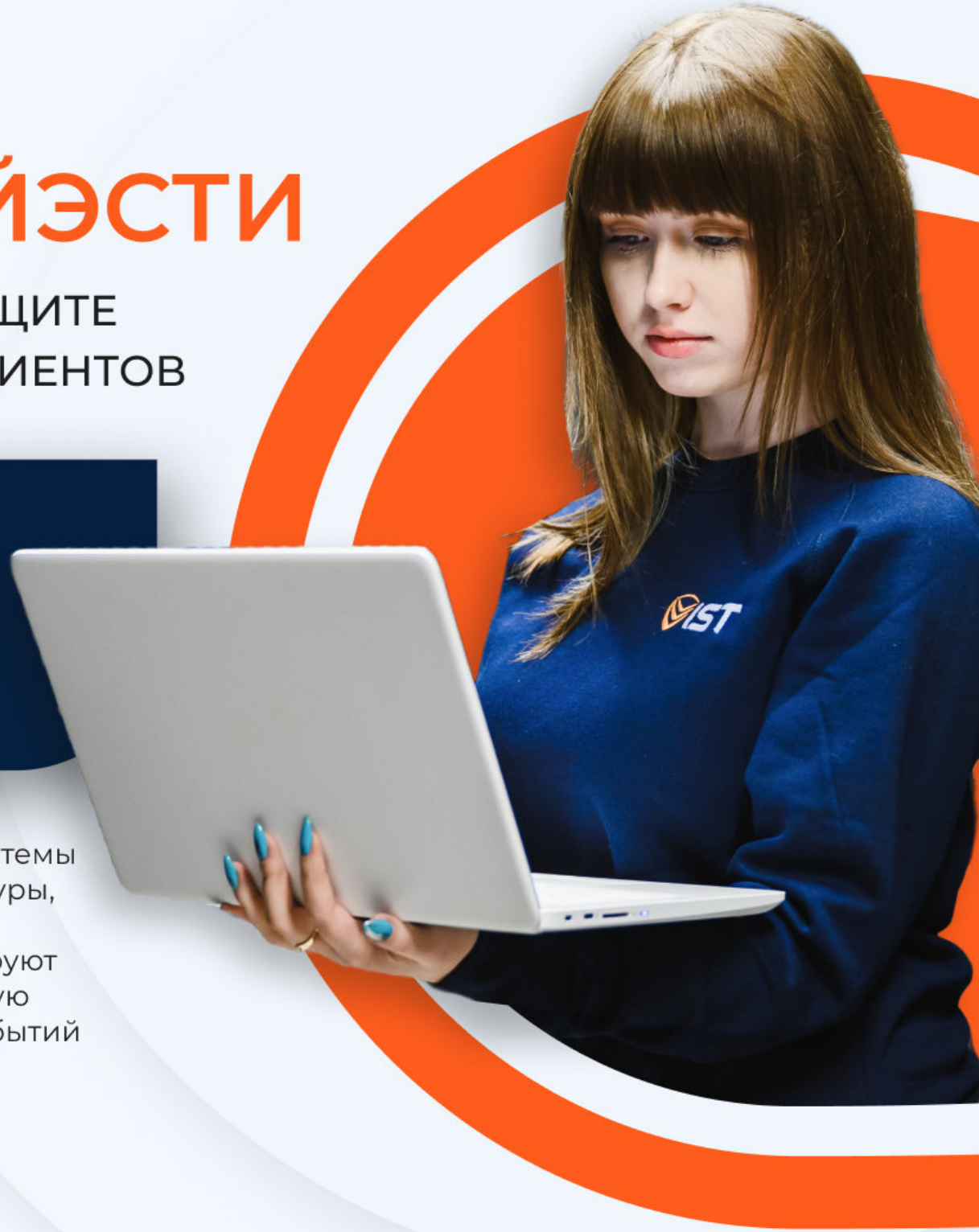


КОМПАНИЯ АЙЭСТИ

ПРЕДОСТАВЛЯЕТ УСЛУГИ ПО ЗАЩИТЕ ЦИФРОВЫХ АКТИВОВ СВОИХ КЛИЕНТОВ

Мы помогаем организациям

определить свои критические бизнес-процессы, а также возможные события, наступление которых приведет к разрушительным или фатальным для организации последствиям



Наши специалисты выявят информационные системы и элементы телекоммуникационной инфраструктуры, которые связаны с данными бизнес-процессами или событиями, определят уязвимости, спроектируют и внедрят систему кибербезопасности, нацеленную на невозможность наступления недопустимых событий

СОТРУДНИЧЕСТВО С НАМИ — ЭТО УВЕРЕННОСТЬ В БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Квалификация наших специалистов, опыт
и производственная база соответствует требованиям

- ФСБ России
- МЧС России
- ФСТЭК России

Подтверждено соответствующими лицензиями

МЫ ВЫПОЛНЯЕМ:

Экспертный аудит

защищенности информационных систем и телекоммуникационной инфраструктуры

Проектирование

систем защиты информации

Поставку, внедрение и техническое сопровождение

средств и систем защиты информации

Построение

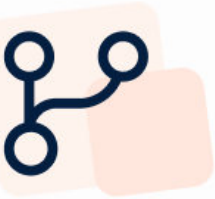
систем кибербезопасности АСУ ТП

Консультирование

по законодательству в сфере информационной безопасности

Аутсорсинг

информационной безопасности для организации любого масштаба



Построение

процесса безопасной разработки программного обеспечения

Экспертное сопровождение

для получения лицензий ФСТЭК и ФСБ

ЭКСПЕРТНЫЙ АУДИТ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аудит защищенности

Это независимое исследование состояния информационных систем, рабочих станций, сетевого оборудования и средств защиты информации, поиск уязвимостей сетевой инфраструктуры с помощью различных инструментов и методов, сбор логов с узлов сети, проведение углубленного анализа сетевой архитектуры и настроек ее элементов

По итогам аудита

будет предоставлено **полное описание систем и сетей,** выявленных уязвимостей и рекомендации экспертов ИБ по закрытию слабых мест инфраструктуры, реализация которых поможет обеспечить:

- непрерывность важных для организации процессов
- повысить киберустойчивость критических информационных систем

ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Проектирование системы защиты информации позволяет обеспечить комплексный подход к выбору мер и средств защиты информации

При составлении проекта:

- определяются субъекты и объекты защиты
- определяются методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам, подлежащие реализации в информационной системе
- выбираются меры защиты информации, подлежащие реализации в системе защиты информации;
- определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации
- определяется структура системы защиты информации, включая состав, количество и места размещения ее элементов
- осуществляется выбор средств защиты информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы
- определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации
- определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями

ПОСТАВКА, ВНЕДРЕНИЕ И ТЕХНИЧЕСКОЕ СОПРОВОЖДЕНИЕ СРЕДСТВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

АйЭсТи

Является авторизованным партнером большинства российских производителей средств защиты информации (СрЗИ). Это означает, что **мы сможем грамотно подобрать состав СрЗИ под задачи Клиента, предоставить лучшие цены и обеспечить своевременную поставку**

Наши специалисты

Регулярно обучаются и подтверждают квалификацию в авторизованных учебных центрах производителей средств защиты информации. Независимо от того, где были приобретены СрЗИ, мы **поможем их грамотно установить и настроить,** с учетом их взаимодействия с окружающим программным обеспечением, технологиями и архитектурой сети

Однажды установленные и настроенные СрЗИ требуют регулярного обновления версий, сигнатур, баз правил. Окружение, в котором работают СрЗИ также нестатично. Наши специалисты **помогут поддерживать в актуальном состоянии версии и настройки СрЗИ, проконсультируют по вопросам их эксплуатации**

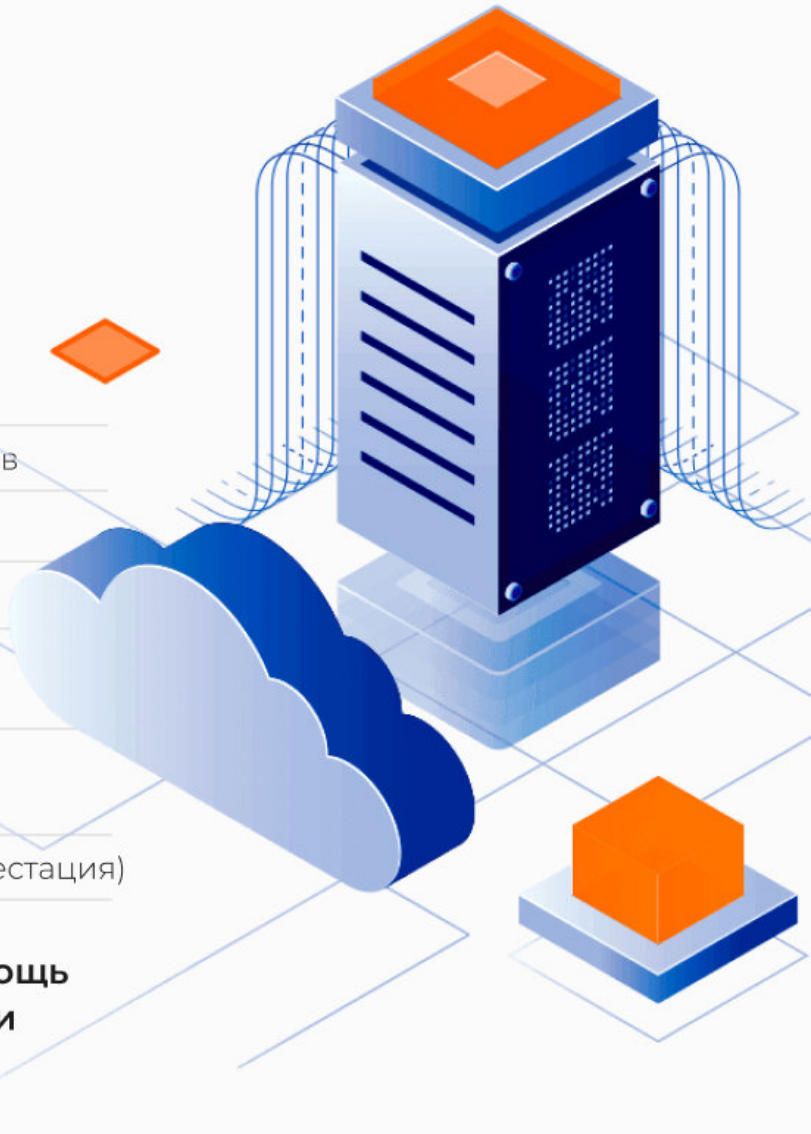
ПОСТРОЕНИЕ СИСТЕМ КИБЕРБЕЗОПАСНОСТИ АСУ ТП

АСУ ТП

Обычно имеют более высокие уровни риска по сравнению с корпоративными информационными системами. Нарушение работы АСУ ТП может привести к выпуску бракованной продукции, остановке производственных линий или выходу из строя оборудования, и, как следствие, к серьезным экономическим потерям

При построении системы кибербезопасности АСУ ТП мы поможем:

- провести обследование АСУ ТП и определить уровень значимости её элементов
- определить угрозы и возможные уязвимости
- сформировать требования к защите информации в АСУ ТП
- спроектировать систему защиты АСУ ТП и разработать эксплуатационную документацию на систему защиты информации
- внедрить систему защиты информации (реализовать организационное и техническое обеспечение защиты АСУ ТП)
- провести приемочные испытания объекта и его подсистемы безопасности (аттестация)



На дальнейших этапах функционирования АСУ ТП АйЭсТи окажет помощь в поддержании действующей системы защиты в актуальном состоянии

АУТСОРСИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОРГАНИЗАЦИЙ ЛЮБОГО МАСШТАБА

Обеспечение информационной безопасности — процесс непрерывный, требующий профильных знаний и опыта

Передача части функций службы информационной безопасности актуальна, если у организации присутствует:

- Нехватка штатного персонала, оптимизация штата службы ИБ
- Потребность поддержки в режиме 24/7
- Необходимость в экспертизе узкопрофильных специалистов по ИБ
- Потребность в быстром построении системы ИБ
- Необходимость сокращения издержек на обеспечение информационной безопасности

Аутсорсинг информационной безопасности от АйЭсТи

сократит затраты на ИБ, решит проблему нехватки штатных специалистов и их компетенций, повысит уровень защищенности информационно-телекоммуникационной инфраструктуры организации, обеспечивает выполнение требований законодательства по ИБ и успешное прохождение проверок контролирующих органов

ЭКСПЕРТНОЕ СОПРОВОЖДЕНИЕ ДЛЯ ПОЛУЧЕНИЯ ЛИЦЕНЗИЙ ФСТЭК И ФСБ

Лицензии ФСТЭК и ФСБ

Необходимы организациям для оказания услуг в сфере технической защиты конфиденциальной информации и услуг с использованием шифровальных (криптографических) средств. Процесс выполнения требований законодательства и подготовки пакета документов для получения лицензий — сложный и трудоемкий процесс

АйЭсТи

- Окажет комплекс услуг по подготовке к получению лицензий в рамках: Постановлений Правительства РФ:№79, №313 и №171
- Мы проконсультируем по подбору технических средств и персонала, поможем оборудовать и проведем аттестацию выделенных помещений, разработаем шаблоны необходимых документов
- Наши специалисты окажут экспертное сопровождение при возникновении вопросов регуляторов, помогут обработать замечания и сделают получение лицензий более понятным и прозрачным процессом

КОНСУЛЬТИРОВАНИЕ ПО ЗАКОНОДАТЕЛЬСТВУ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Законодательство и нормативная база по информационной безопасности достаточно обширны и сложны для понимания. При этом они нестатичны, в них достаточно часто вносятся изменения. Наши специалисты на регулярной основе посещают форумы и конференции, изучают аналитические и новостные материалы, имеют большой опыт реализации проектов, связанных с выполнением требований законодательства по ИБ, постоянно общаются с ФСТЭК и ФСБ по рабочим вопросам

Если вам необходима исчерпывающая или дополнительная информация, а также помощь компетентных консультантов, **мы готовы оказать вам услуги:**

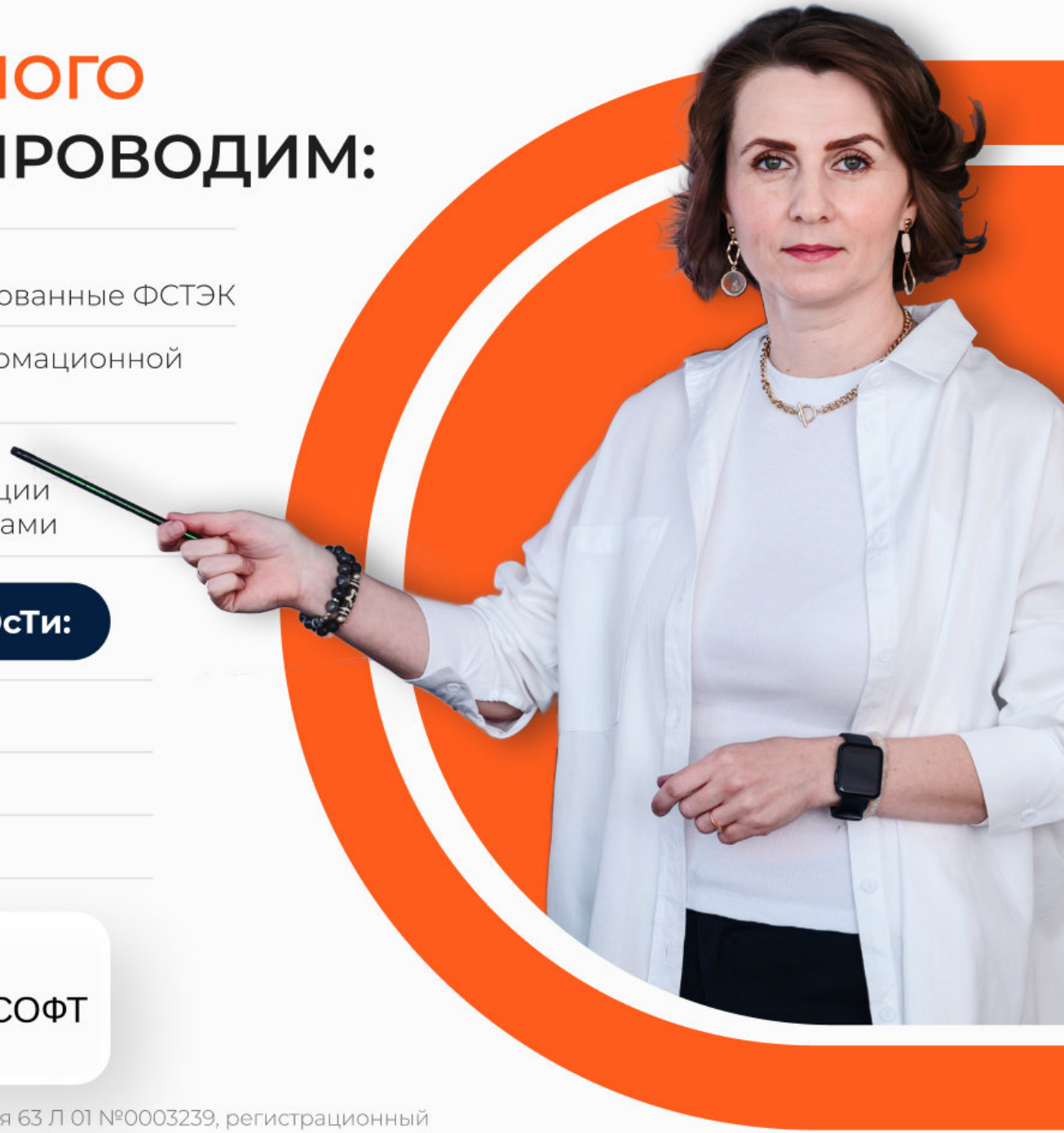
- по вопросам обработки и защиты персональных данных
- безопасности объектов КИИ
- защиты государственных и финансовых информационных систем
- коммерческой тайны
- взаимодействия с контролирующими органами (Роскомнадзор, ФСТЭК России, ФСБ)
- разработки стратегий и концепций информационной безопасности
- разработки организационно-распорядительной документации по ИБ

На регулярной основе АйЭсТи может информировать, что изменилось в законодательстве по ИБ, как это влияет на организацию, что необходимо делать, и какие риски несет игнорирование новых требований

IST
УЧЕБНЫЙ ЦЕНТР

НА БАЗЕ СОБСТВЕННОГО УЧЕБНОГО ЦЕНТРА ПРОВОДИМ:

- Курсы профессиональной переподготовки по информационной безопасности, согласованные ФСТЭК
- Курсы повышения квалификации по информационной безопасности, согласованные ФСТЭК
- Авторизованные производителями курсы по работе со средствами защиты информации и отечественными операционными системами

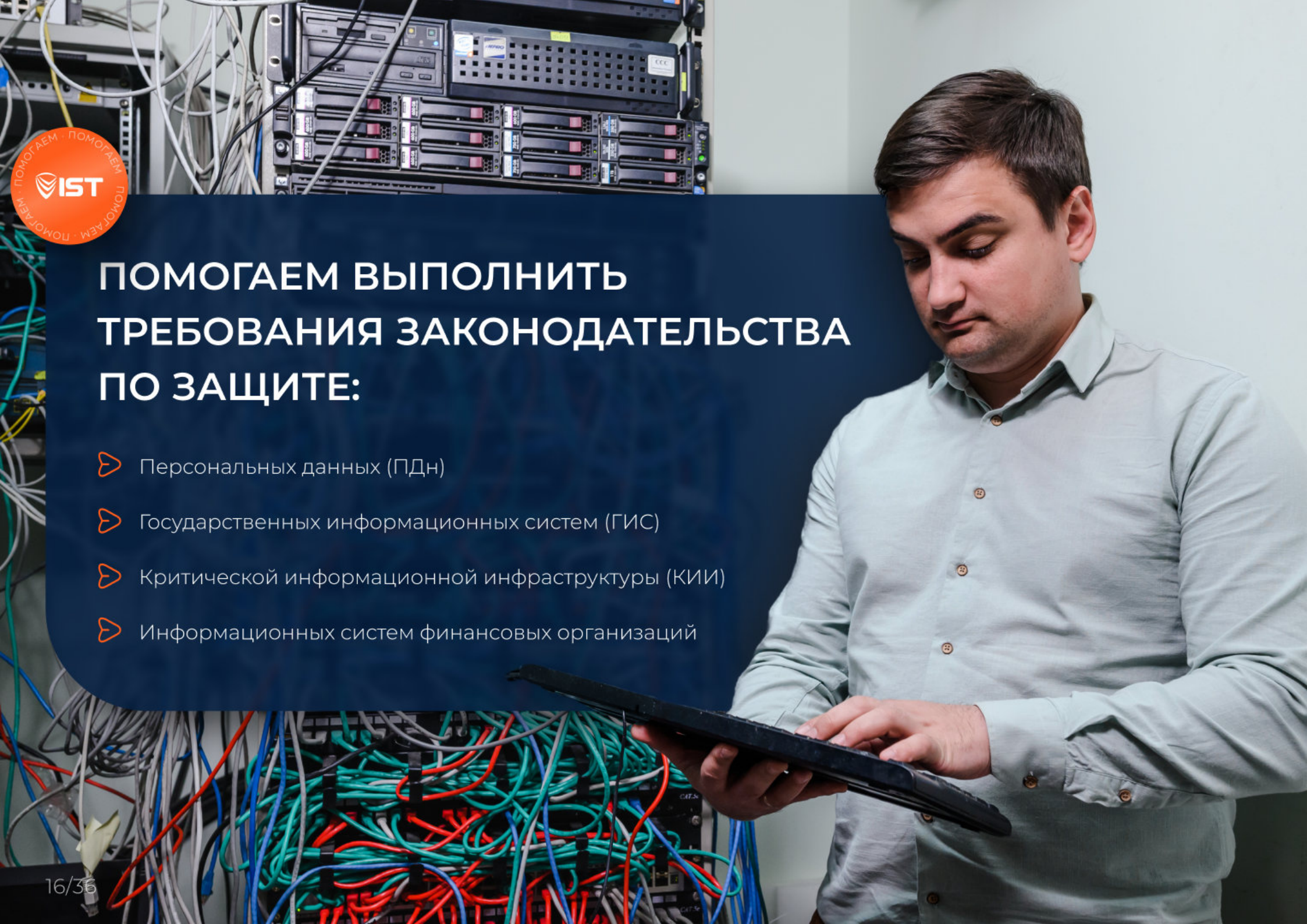


Преимущества Учебного центра АйЭсТи:

- Программы согласованы ФСТЭК России
- Актуальные наполнения курсов
- Преподаватели-практики

infotecs® ASTRALINUX® РЕДСОФТ

* Лицензия на образовательную деятельность: серия 63 Л 01 №0003239, регистрационный номер 7471 от 02.04.2020 г., выданной Министерством образования и науки Самарской области



ПОМОГАЕМ ВЫПОЛНИТЬ ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА ПО ЗАЩИТЕ:

- Персональных данных (ПДн)
- Государственных информационных систем (ГИС)
- Критической информационной инфраструктуры (КИИ)
- Информационных систем финансовых организаций

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Что такое персональные данные (ПДн)?

- **Персональные данные -** это любая информация, с помощью которой можно идентифицировать личность человека

Зачем обеспечивать защиту персональных данных?

- Любая организация, обрабатывающая персональные данные (то есть осуществляющая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение персональных данных) является Оператором

В соответствии с законодательством Российской Федерации каждый Оператор обязан обеспечивать защиту персональных данных

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Чем мы можем быть полезны при построении системы защиты персональных данных?

Построение системы защиты ПДн объемный и полный нюансов процесс, поэтому **наши специалисты помогут:**

- провести экспертный аудит и выявить информационные системы, в которых ведется обработка ПДн
- определить перечень персональных данных и присвоить уровень защищенности информационных систем персональных данных
- сформировать требования к построению системы защиты (проектирование системы защиты)
- реализовать организационное и техническое обеспечение защиты персональных данных

На дальнейших этапах функционирования ИСПДн **окажем помощь в поддержании действующей системы защиты в актуальном состоянии**

А также мы **оказываем сопровождение организации в части обработки ПДн** при внесении изменений в законодательство в сфере информационной безопасности (консультируем, информируем и т.д.)

ЗАЩИТА ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Что такое государственные информационные системы (ГИС)?

- **Государственные информационные системы** – это информационные системы, которые создаются в целях выполнения государственными органами своих функций

Зачем обеспечивать защиту государственных информационных систем?

- В соответствии с Федеральным законом от 27.07.2006 N 149- ФЗ «Об информации, информационных технологиях и о защите информации» государственный орган, регламентирующий работу ГИС (Оператор ГИС) обязан обеспечить защиту ГИС от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий

ЗАЩИТА ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

#2

Чем мы можем быть полезны при построении системы защиты персональных данных?

Построение системы защиты ГИС является одним из важнейших этапов при создании ГИС и предполагает привлечение организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации. **Наши специалисты помогут:**

- провести аудит и определить, является ли данная информационная система государственной
- определить масштаб информационной системы, уровень значимости обрабатываемой в ней информации и определить класс защищенности ГИС
- сформировать требования к построению системы защиты (проектирование системы защиты)
- организовать взаимодействие с Регуляторами (ФСБ и ФСТЭК) при согласовании Модели угроз безопасности информации и Технического задания на создание системы защиты
- разработать эксплуатационную документацию
- реализовать организационное и техническое обеспечение защиты ГИС

Ввод в эксплуатацию ГИС допускается только после проведения аттестации на соответствие требованиям по защите информации. Данные работы может проводить только организация, имеющая лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации, и такая лицензия у нас есть

А также мы можем сопровождать систему защиты ГИС **на всем протяжении ее жизненного цикла**

БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Что такое критическая информационная инфраструктура (КИИ)?

- **Критическая информационная инфраструктура** представляет собой комплекс из объектов КИИ и сетей электросвязи, используемых для организации взаимодействия таких объектов

Что такое объект КИИ?

- **Объекты КИИ** – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры

Кто является субъектом КИИ?

- **Субъекты КИИ** – организации, которым принадлежат информационные системы, функционирующие в сферах здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а также организации, которые обеспечивают взаимодействие указанных систем или сетей

БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

#2

Чем мы можем быть полезны при построении систем защиты критической информационной инфраструктуры?

Вопросы, возникающие при обеспечении безопасности КИИ регулируются Федеральным законом от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и иными нормативными актами, исполнение которых является обязательным для субъектов КИИ. Если ваша организация является владельцем информационных систем, функционирующих в сферах КИИ, **наши специалисты помогут:**

- провести аудит на предмет выявления объектов КИИ (ОКИИ)
- провести категорирование объектов в соответствии с требованиями нормативных документов
- разработать план подключения к ГосСОПКА и план информирования НКЦКИ
- сформировать требования к построению системы защиты (проектирование системы защиты)
- разработать эксплуатационную документацию на систему защиты ОКИИ
- реализовать организационное и техническое обеспечение защиты ОКИИ
- провести приемочные испытания объекта и его подсистемы безопасности (аттестация)

На всех этапах функционирования ОКИИ мы **окажем помощь** в поддержании действующей системы защиты в актуальном состоянии, **проинформируем и проконсультируем** при внесении изменений в законодательство в сфере информационной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ

Какие организации относятся к финансовым?

- Операторы по переводу денежных средств;
- Банковские платежные агенты(субагенты);
- Операторы услуг информационного обмена;
- Поставщики платежных приложений;
- Операторы платежных систем;
- Операторы услуг платежной инфраструктуры
- Банки
- Небанковская кредитная организация, имеющая право на осуществление переводов денежных средств без открытия банковских счетов и связанных с ними иных банковских операций;
- Расчетная небанковская кредитная организация; небанковская кредитная организация, осуществляющая депозитно-кредитные операции;
- Небанковская кредитная организация — центральный контрагент;
- Некредитные финансовые организации согласно статье 76.1, Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ

Зачем нужна информационная безопасность в финансовых организациях?

- **Обеспечение безопасности информации** в финансовых организациях регламентируется группой Федеральных законов, Приказами ФСБ и ФСТЭК, комплексом Стандартов Банка России, ГОСТов

- **Весь свод нормативной базы включает в себя** требования в сфере персональных данных, в сфере критической информационной инфраструктуры и требования соответствия Положениям Центрального банка

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ

#3

Чем мы можем быть полезны при построении системы защиты информации в финансовых организациях?

Для реализации требований законодательства необходимо привлекать организацию с лицензией ФСТЭК на деятельность по технической защите конфиденциальной информации. У нас такая лицензия есть. **Наши сотрудники смогут:**

- провести экспертный аудит с целью консультирования и составления рекомендаций по созданию или модернизации системы защиты
- сформировать требования к защите информации в финансовой организации
- разработать организационно-распорядительную документацию
- реализовать организационное и техническое обеспечение защиты информации согласно ГОСТ 57580.1-2017, ГОСТ 57580.3-2022, ГОСТ 57580.4-2022
- провести оценку соответствия Требованиям по защите информации согласно ГОСТ Р 57580.2-2018

Также мы создаем и модернизируем удостоверяющие центры, реализуем защиту онлайн-сервисов, помогаем подключиться к Единой биометрической системе (ЕБС). Оказываем поддержку действующей системы защиты информации на всех этапах функционирования информационных систем в финансовых организациях, информируем и консультируем при внесении изменений в законодательство в сфере информационной безопасности

В РАБОТЕ С КЛИЕНТАМИ

МЫ ПРИДЕРЖИВАЕМСЯ ГИБКОГО И НЕФОРМАЛИЗОВАННОГО ПОДХОДА

Для нас важно предоставить клиенту наиболее оптимальное решение, соответствующее его потребностям. Мы предлагаем только то, в чем уверены сами, и что наши специалисты проверили на практике

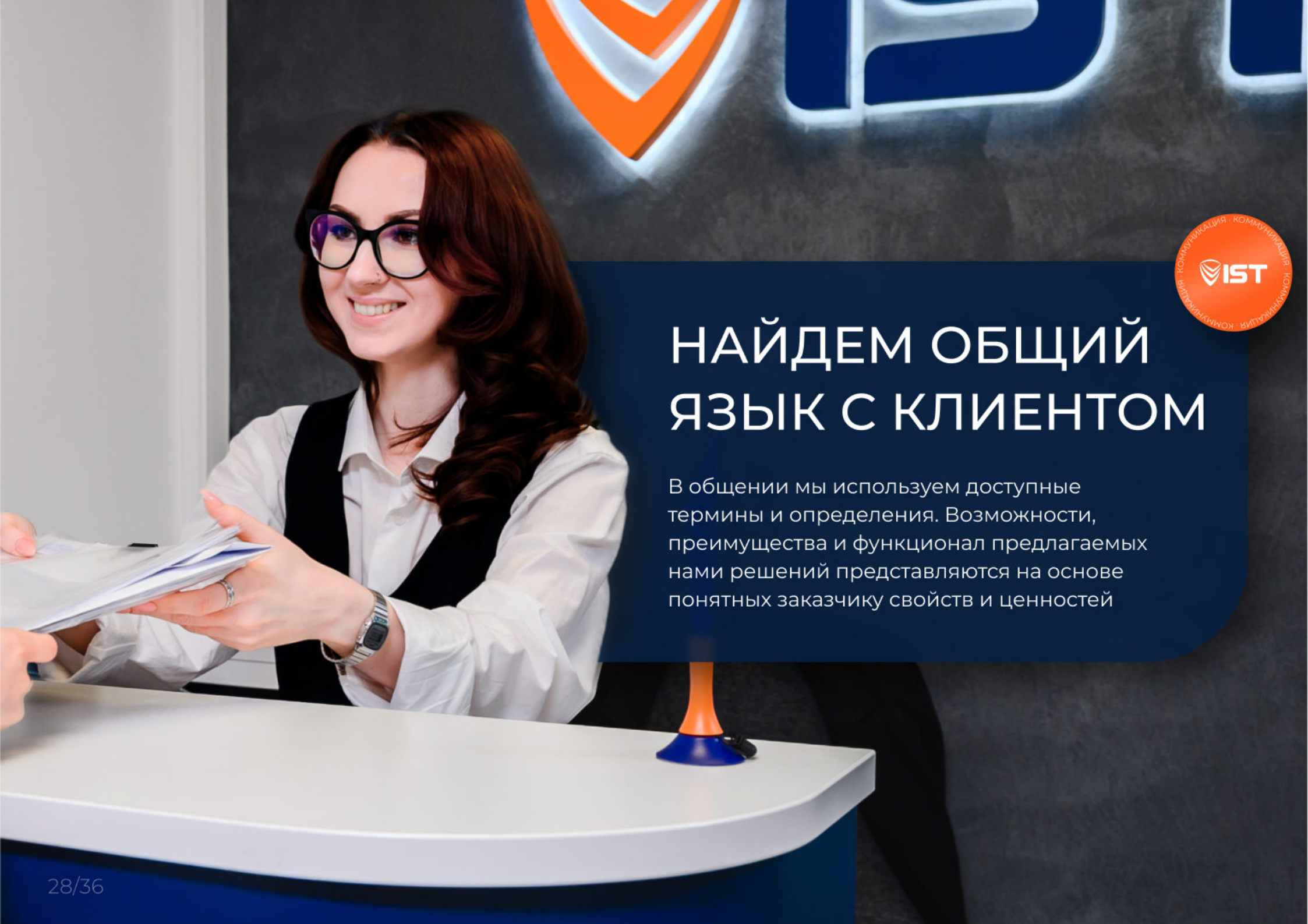
Политика компании: долгосрочные и доверительные отношения с заказчиками, оказание помощи и поддержки постоянным клиентам

НАШИ СПЕЦИАЛИСТЫ

— ВЫСОКОКВАЛИФИЦИРОВАННЫЕ ПРОФЕССИОНАЛЫ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Благодаря опыту и метакомпетенциям наша команда может решать нестандартные задачи по:

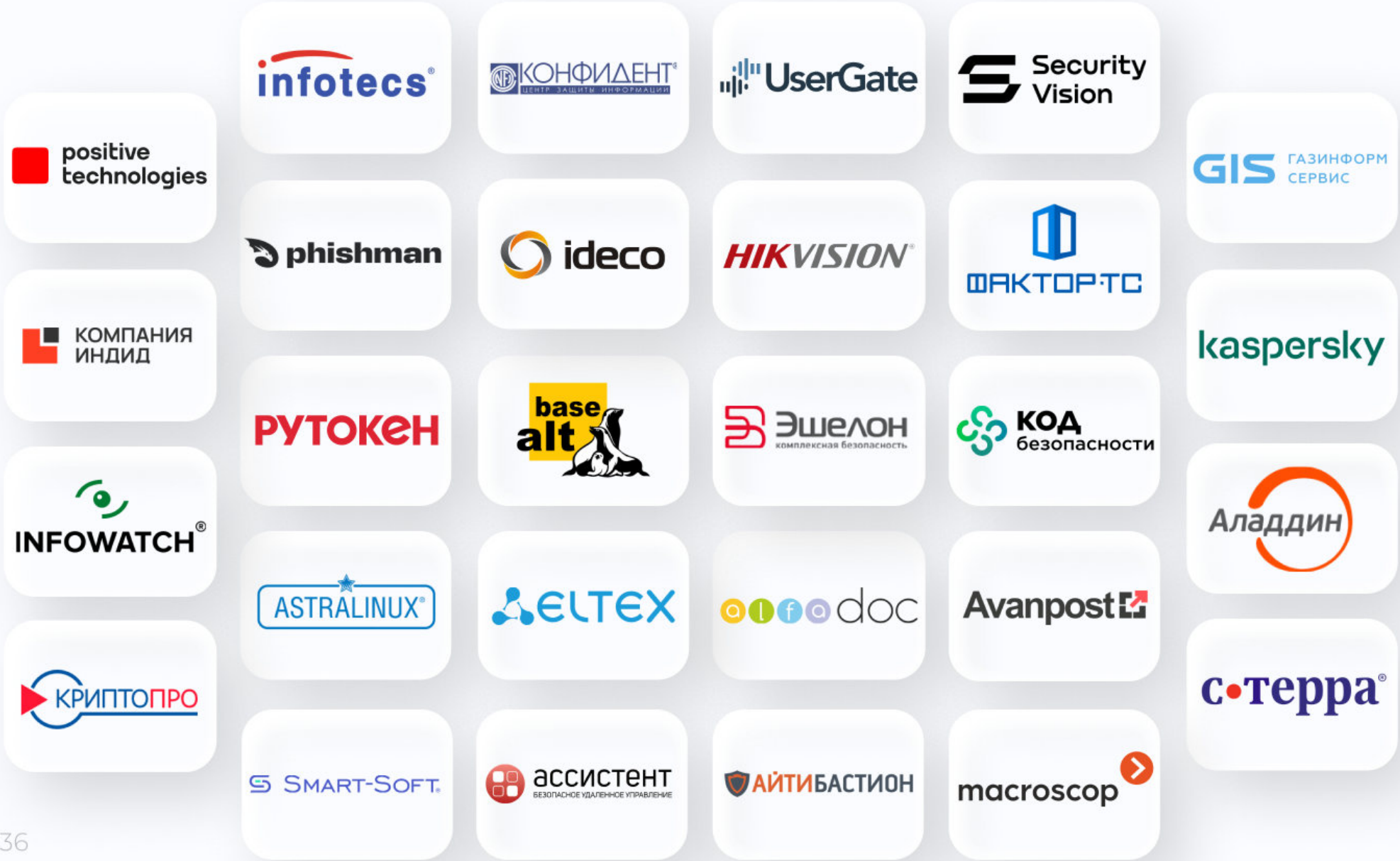
- аудиту защищенности информационно-телекоммуникационной инфраструктуры
- подбору и внедрению средств защиты информации
- расследованию инцидентов информационной безопасности



НАЙДЕМ ОБЩИЙ ЯЗЫК С КЛИЕНТОМ

В общении мы используем доступные термины и определения. Возможности, преимущества и функционал предлагаемых нами решений представляются на основе понятных заказчику свойств и ценностей

БОЛЕЕ 40 ВЕНДОРОВ
В ПАРТНЕРСКОМ ПОРТФЕЛЕ



НАШИ СТАТУСЫ У ВЕНДОРОВ:

01

Золотой партнер
UserGate 2022

UserGate

02

Платиновый партнер
Конфидент 2023

КОНФИДЕНТ
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

03

Платиновый партнер
Infotecs 2023

infotecs®

04

Уровень Professional Advanced и Лучший партнер
Positive Technologies в ПФО 2023

positive technologies

МНОГОЛЕТНИЙ ОПЫТ РАБОТЫ
С ОТЕЧЕСТВЕННЫМИ ИБ РЕШЕНИЯМИ

Работая преимущественно с отечественными программными продуктами и оборудованием, мы накопили знания, которые позволяют нам **реализовывать проекты по импортозамещению максимально безболезненно для наших заказчиков**

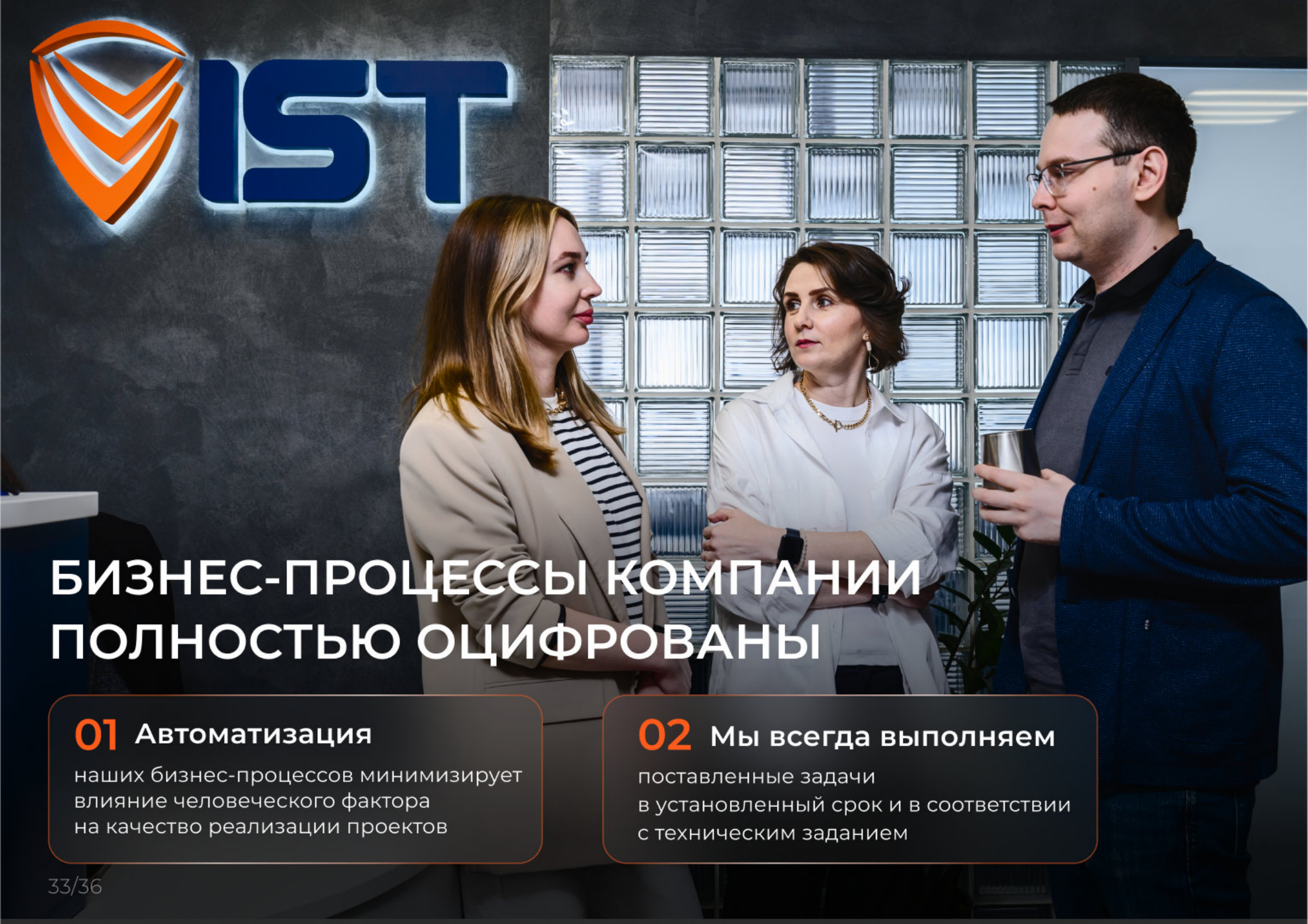
ПРИМЕНЯЕМ ЛУЧШИЕ ПРАКТИКИ ИЗ ОТРАСЛИ ИБ

Компания всегда идет в ногу со временем

01 **Наши специалисты посещают все крупные конференции** по информационной безопасности, форумы, партнерские мероприятия

02 **Мы изучаем новые решения вендоров,** отслеживаем изменения законодательства, анализируем мнения экспертов отрасли

03 **С 2017 года являемся организатором ежегодной конференции** «Технологии информационной безопасности» в Самаре



БИЗНЕС-ПРОЦЕССЫ КОМПАНИИ ПОЛНОСТЬЮ ОЦИФРОВАНЫ

01 Автоматизация

наших бизнес-процессов минимизирует влияние человеческого фактора на качество реализации проектов

02 Мы всегда выполняем

поставленные задачи в установленный срок и в соответствии с техническим заданием

МИНИМАЛЬНОЕ ВРЕМЯ РЕАКЦИИ НА ЗАПРОСЫ

01 Скорость ответа на запросы по подбору решений или подготовке коммерческих предложений 1-2 дня

02 Вам не требуется заполнять объемные анкеты с непонятными параметрами. Наши специалисты проведут интервью на основе простых вопросов и определят ваши потребности

РАБОТАЕМ В РЕГИОНАЛЬНЫХ РАСЦЕНКАХ

01

Мы реализуем проекты по всей России

02

Но наши цены ниже, чем у столичных компаний, **при таком же качестве услуг,** поскольку наши офисы находятся в регионах, и у нас региональные издержки

Консультация

ПОЛУЧИТЕ БЕСПЛАТНУЮ КОНСУЛЬТАЦИЮ ОТ НАШИХ СПЕЦИАЛИСТОВ

Оставить заявку

Записаться на курс

8 800 700 19 56

info@zaschita-it.ru