



Партнерская база знаний по ИКС

Руководство по продукту, подбору и продажам

Цель документа: помочь партнеру уверенно разобраться в ИКС, корректно подобрать решение и провести заказчика от первого контакта до внедрения и продления. Надежная техническая квалификация защищает репутацию партнера, а работа с продлениями и развитием заказчиков создает повторный доход.



Оглавление

1. [Знакомство с продуктом](#)
2. [Возможности ИКС](#)
3. [Требования регуляторов](#)
4. [Целевые заказчики и сценарии применения](#)
5. [Подбор решения](#)
6. [Лицензирование](#)
7. [Процесс продажи ИКС](#)
8. [Скрипты и инструменты продаж](#)
9. [Работа с возражениями](#)
10. [Техническая поддержка](#)
11. [Коммерческие и маркетинговые материалы](#)
12. [Словарь терминов](#)
13. [Контроль знаний партнёра](#)
14. [Ответы к контролю знаний](#)



1. Знакомство с продуктом

1.1 Что такое ИКС и какие задачи он решает

ИКС — российский программный продукт для защиты сети организации и управления интернет-трафиком. Полное название — «Интернет Контроль Сервер».

Проще всего представить ИКС как контрольно-пропускной пункт между интернетом и внутренней сетью. Через него проходит сетевой трафик организации. ИКС проверяет соединения, применяет заданные администратором правила, разрешает необходимые действия и блокирует запрещённые.

Заказчик обычно ищет не межсетевой экран как таковой, а решение конкретных проблем: защитить сеть, ограничить доступ к сайтам, подключить филиалы, заменить зарубежный продукт или выполнить требования к защите информации. Поэтому сначала необходимо выяснить задачи заказчика и только после этого подбирать функции и конфигурацию ИКС.

1.1.1 Основные задачи

Задача заказчика	Как помогает ИКС
Защитить сеть от внешних угроз	Контролирует входящие и исходящие соединения, блокирует запрещённый трафик и выявляет признаки сетевых атак
Управлять доступом сотрудников в интернет	Устанавливает разные правила для пользователей, групп, сайтов, приложений, протоколов и времени работы
Ограничить опасные и нежелательные ресурсы	Блокирует отдельные адреса, категории сайтов, приложения, типы файлов и другой нежелательный контент
Подключить удалённых сотрудников	Создаёт защищённые VPN-соединения; для дополнительной защиты может использоваться двухфакторная аутентификация
Объединить офисы и филиалы	Связывает удалённые сети через VPN-каналы
Разделить сеть на участки	Контролирует обмен данными между рабочими местами, серверами, гостевой сетью, камерами и другими сегментами
Распределить интернет-канал	Ограничивает скорость, назначает приоритет важному трафику и поддерживает несколько каналов связи
Понять, что происходит в сети	Ведёт журналы и формирует отчёты о соединениях, действиях пользователей и событиях безопасности
Повысить доступность сервисов	Поддерживает резервные интернет-каналы и отказоустойчивую конфигурацию из двух серверов
Проверять трафик на вредоносные объекты	Использует дополнительные антивирусные модули; такая проверка дополняет, но не заменяет защиту рабочих станций

Задача заказчика	Как помогает ИКС
Выполнить требования к защите информации	Предоставляет сертифицированную редакцию ИКС ФСТЭК для тех систем, где она может применяться
Заменить зарубежное или устаревшее решение	Предлагает российский продукт с русскоязычным интерфейсом, документацией и технической поддержкой

NGFW ИКС также может выполнять дополнительные задачи: обеспечивать работу корпоративной электронной почты и IP-телефонии, взаимодействовать с доменной инфраструктурой и передавать события в системы мониторинга и информационной безопасности.

Использовать все возможности одновременно необязательно. Состав функций определяется задачами и инфраструктурой конкретного заказчика.

1.1.2 Что важно запомнить

ИКС становится единой точкой контроля сетевого трафика. Он помогает защищать сеть, управлять доступом в интернет, подключать сотрудников и филиалы, контролировать события и собирать данные для анализа.

При продаже лучше говорить не «в ИКС есть функция», а «с помощью этой функции заказчик решит конкретную задачу».

1.2 Кому подходит ИКС

Основная аудитория ИКС — организации примерно от 50 до 1500 пользователей. Однако численность является только ориентиром: важнее задачи, инфраструктура и требования к защите информации.

1.2.1 Типовые заказчики

Коммерческие компании. ИКС подходит организациям, которым требуется защитить сеть, управлять доступом сотрудников в интернет, организовать удалённую работу или заменить зарубежный межсетевой экран. Особенно востребовано понятное решение с русскоязычной поддержкой там, где нет большого отдела информационной безопасности.

Государственные и муниципальные организации. Им может потребоваться сертифицированное средство для защиты конкретной информационной системы. В таком проекте рассматривается ИКС ФСТЭК, но необходимость его применения определяется требованиями к системе, а не только формой собственности заказчика.

Образовательные учреждения. Школам, колледжам и вузам важно ограничивать нежелательные сайты, разделять права сотрудников и учащихся, контролировать использование интернета и защищать внутренние ресурсы.

Медицинские организации. Больницам, поликлиникам, лабораториям и медицинским центрам необходимо защищать сети, в которых обрабатываются персональные и медицинские данные, разделять сегменты и безопасно связывать филиалы.

Торговые сети и другие распределённые организации. ИКС помогает объединять

площадки через VPN, управлять интернет-доступом и использовать резервные каналы связи.

Промышленные предприятия. Продукт может контролировать обмен данными между офисной и технологической сетью, серверами, камерами и оборудованием. Если защищается значимый объект КИИ, АСУ ТП или другая регулируемая система, рассматривается ИКС ФСТЭК.

1.2.2 Признаки потенциальной потребности

Стоит предложить консультацию, демонстрацию или тестирование ИКС, если заказчик:

- использует зарубежный продукт или решение с прекращённой поддержкой;
- недоволен стоимостью или сложностью действующего межсетевого экрана;
- открывает офисы, расширяет сеть или объединяет филиалы;
- подключает удалённых сотрудников;
- хочет контролировать сайты, приложения и использование интернет-канала;
- планирует разделить сеть на изолированные сегменты;
- нуждается в резервировании интернет-доступа;
- должен применять сертифицированные средства защиты;
- хочет сократить количество отдельных программ;
- ищет российское решение с поддержкой на русском языке.

Отрасль сама по себе не определяет выбор продукта. Например, медицинской организации ИКС ФСТЭК требуется не потому, что она медицинская, а потому, что конкретная система обрабатывает защищаемую информацию и для неё установлены соответствующие требования.

1.3 Что такое межсетевой экран и NGFW

Межсетевой экран контролирует обмен данными между сетями. Он проверяет соединения по установленным правилам, разрешает необходимые и блокирует запрещённые.

Например, межсетевой экран может разрешить сотрудникам доступ в интернет, запретить внешнее подключение к внутреннему серверу и ограничить обмен данными между гостевой и корпоративной сетью.

NGFW — межсетевой экран нового поколения. Помимо базового контроля соединений он глубже анализирует трафик и может учитывать:

- пользователя или группу;
- сайт, приложение и протокол;
- содержимое и тип передаваемых данных;
- признаки сетевой атаки;
- заданную политику безопасности.

В зависимости от конфигурации NGFW также фильтрует интернет-ресурсы, обнаруживает атаки, проверяет трафик на вредоносные объекты и создаёт VPN-соединения.

Простыми словами, обычный межсетевой экран проверяет, откуда и куда направлено соединение, а NGFW дополнительно понимает, кто его создаёт, какое приложение используется и нет ли признаков угрозы.

NGFW ИКС относится к межсетевым экранам нового поколения.

1.4 Место ИКС в инфраструктуре

Обычно ИКС устанавливается на границе между интернетом и локальной сетью. Чтобы продукт мог контролировать соединения, необходимый трафик должен проходить через него.

1.4.1 Типовые сценарии использования

ИКС как основной шлюз. Продукт напрямую подключается к интернету и становится основной точкой выхода для компьютеров и других устройств. Это базовая схема для одного офиса.

ИКС после маршрутизатора. В этом случае ИКС становится участником сети. Трафик от устройств обрабатывается межсетевым экраном. Далее попадает на маршрутизатор и в интернет. Важно исключить обходные подключения, через которые трафик сможет идти мимо ИКС.

Разделение внутренней сети. ИКС устанавливает разные правила для рабочих мест, серверов, гостевой сети, камер, беспроводных устройств и технологического оборудования. Сегментация помогает ограничить доступ и распространение атаки между участками инфраструктуры.

Объединение филиалов. ИКС устанавливается на нескольких площадках, которые связываются защищёнными VPN-каналами. Филиалы получают доступ только к разрешённым ресурсам головного офиса.

Подключение удалённых сотрудников. Пользователь подключается к корпоративной сети по VPN из дома или командировки. Ему следует предоставлять доступ только к ресурсам, необходимым для работы.

Отказоустойчивая схема. Для критичных сервисов могут использоваться резервные интернет-каналы и два сервера ИКС. При отказе основного канала или сервера работу принимает резервный.

Универсального сценария нет. Конфигурация зависит от структуры сети, количества площадок, требуемой производительности и допустимого времени простоя. Если инфраструктура сложная, схему необходимо подбирать вместе с техническим специалистом.

1.5 Редакции и варианты поставки ИКС

При подборе решения нужно последовательно ответить на два вопроса:

1. Нужна обычная или сертифицированная редакция?
2. Заказчик установит программу на свою платформу или ему нужен готовый программно-аппаратный комплекс?

1.5.1 Редакции

NGFW ИКС предназначен для решения общих задач сетевой защиты, когда сертификат ФСТЭК не требуется. Он позволяет контролировать трафик и интернет-доступ, обнаруживать атаки, создавать VPN, управлять каналами связи, вести журналы и использовать дополнительные сервисы.

ИКС ФСТЭК — сертифицированная редакция для информационных систем, в которых проектом предусмотрен сертифицированный межсетевой экран или система обнаружения вторжений. Возможность применения определяется областью сертификата и требованиями конкретной системы.

Важно! Редакция NGFW ИКС не становится сертифицированной из-за того, что у производителя есть ИКС ФСТЭК.

1.5.2 Варианты поставки

Программная поставка. Заказчик получает программное обеспечение и устанавливает его на совместимый физический сервер или виртуальную машину. В этом случае необходимо правильно подобрать ресурсы и проверить совместимость платформы. Для ИКС ФСТЭК дополнительно учитываются ограничения сертифицированной конфигурации.

Программно-аппаратный комплекс (ПАК). Заказчик получает аппаратную платформу с установленным ИКС. Этот вариант подходит, если он не хочет самостоятельно подбирать сервер, желает приобрести программу и оборудование в составе одного решения или должен использовать предусмотренный проектом сертифицированный комплекс.

Требования заказчика	Подходящий вариант
Сертификат не требуется, совместимая платформа уже есть	Программная поставка NGFW ИКС
Сертификат не требуется, нужен готовый комплект	ПАК NGFW ИКС
Требуется сертифицированное средство, допустима программная поставка	Программная поставка ИКС ФСТЭК в предусмотренной конфигурации
Требуется сертифицированное решение с аппаратной платформой	ПАК ИКС ФСТЭК

1.5.3 Что уточнить у заказчика

1. Требуется ли сертификат ФСТЭК.
2. Для какой информационной системы приобретается ИКС.
3. Есть ли подходящий сервер или виртуальная инфраструктура.
4. Нужна ли поставка оборудования вместе с программным обеспечением.
5. Сколько пользователей и устройств будет работать через ИКС.
6. Какая производительность и какие функции необходимы.
7. Есть ли специальные требования к версии, исполнению и конфигурации средства защиты.

Редакция определяет назначение и наличие сертификации, а вариант поставки — способ размещения продукта. Если требования неясны, решение следует подбирать вместе с техническим специалистом или специалистом по информационной безопасности.

2. Возможности ИКС

ИКС объединяет функции защиты сети, управления доступом в интернет, фильтрации трафика, удалённого подключения, мониторинга и ряд дополнительных сервисов.

Доступность отдельных возможностей зависит от редакции ИКС, выбранной лицензии и подключённых модулей. Перед включением функции в предложение необходимо проверить её наличие для конкретной конфигурации.

2.1 Межсетевое экранирование

Межсетевой экран контролирует обмен данными между интернетом, внутренней сетью и её отдельными сегментами.

Администратор создаёт правила, которые определяют:

- каким пользователям и устройствам разрешено подключение;
- к каким адресам, сервисам и портам можно обращаться;
- какой входящий и исходящий трафик следует разрешить или заблокировать;
- в какие дни и часы действует правило.

Например, можно разрешить сотрудникам доступ в интернет, закрыть неиспользуемые порты, ограничить подключения к отдельному серверу или запретить обращения с нежелательных адресов.

Межсетевой экран является основой защиты сетевого периметра, но его эффективность зависит от корректной настройки правил.

2.2 Управление доступом в интернет

ИКС позволяет устанавливать разные условия доступа в интернет для пользователей, групп и устройств. Можно:

- разрешать или запрещать доступ к сайтам;
- задавать расписание;
- ограничивать скорость;
- учитывать объём использованного трафика;
- применять разные правила к отделам и категориям сотрудников;
- временно отключать доступ отдельному пользователю.

Например, бухгалтерии можно разрешить только необходимые рабочие ресурсы, сотрудникам офиса — более широкий доступ, а гостевым устройствам — отдельный ограниченный выход в интернет.

2.3 Контроль приложений и протоколов

ИКС анализирует трафик и помогает определять используемые сетевые приложения и протоколы.

Это позволяет ограничивать не только отдельные адреса и порты, но и определённые виды трафика. Например, можно контролировать использование мессенджеров, файлообменных сервисов, удалённого доступа и других приложений.

Функция полезна, когда приложение использует разные адреса или стандартные порты и его невозможно надёжно ограничить обычным правилом.

2.4 Контентная фильтрация и фильтрация по категориям

Контентная фильтрация помогает ограничивать доступ к нежелательным интернет-ресурсам. В ИКС можно создавать правила блокировки по:

- адресам сайтов;
- словам и выражениям;
- типам загружаемых файлов;
- расписанию;
- категориям сайтов — при использовании модуля категоризации.

Например, организация может запретить загрузку исполняемых файлов, ограничить развлекательные ресурсы или установить отдельные правила для сотрудников и учащихся.

Для анализа содержимого защищённого HTTPS-трафика требуется его расшифровка. Это необходимо учитывать при проектировании и настройке решения.

2.5 Garnet Web Filter

Garnet Web Filter — дополнительный модуль, который автоматически распределяет сайты по категориям.

Вместо добавления каждого сайта вручную администратор может создать общее правило. Например, запретить ресурсы категорий «Азартные игры» или «Вредоносные сайты», но разрешить образовательные и деловые ресурсы.

Модуль использует регулярно обновляемые данные и анализ содержания веб-страниц. Администратор может использовать собственные правила и списки.

Garnet Web Filter лицензируется отдельно по количеству пользователей и работает совместно с ИКС.

2.6 IDS/IPS и обнаружение сетевых атак

IDS/IPS анализирует сетевой трафик и ищет признаки известных атак, подозрительных действий и попыток использования уязвимостей.

Система может работать в двух основных режимах:

- IDS — обнаруживает подозрительное событие и сообщает о нём;
- IPS — обнаруживает и блокирует трафик, соответствующий заданным правилам.

Для анализа используются правила Suricata. Они определяют, какие признаки необходимо искать в сетевом трафике.

IDS/IPS является дополнительным уровнем защиты, но не гарантирует обнаружение всех атак. Правила необходимо обновлять, а срабатывания — анализировать. Режим блокировки следует включать после проверки, чтобы снизить риск остановки легитимного трафика.

2.7 Поточковая антивирусная проверка

Потоковый антивирус проверяет проходящий через ИКС интернет-трафик и помогает остановить вредоносные объекты до их попадания во внутреннюю сеть.

Функция полезна для проверки загружаемых файлов и другого поддерживаемого содержимого. При обнаружении угрозы передача объекта может быть заблокирована.

Потоковая проверка не заменяет антивирус на рабочих станциях и серверах. Она создаёт дополнительный уровень защиты на сетевом периметре.

Для использования требуется отдельный антивирусный модуль. Его доступность необходимо проверять для выбранной редакции ИКС.

2.8 Антиспам

Антиспам анализирует входящий на ИКС почтовый трафик, и помогает выявлять нежелательные рассылки.

Модуль может применяться:

- для встроенного почтового сервера ИКС;
- при передаче почты через ИКС в режиме SMTP-релея.

Подозрительные сообщения определяются по их содержимому, отправителю и другим признакам. В зависимости от настроек они могут быть отмечены, перенаправлены или заблокированы.

Антиспам является отдельным модулем. Он предназначен для почтового трафика и не защищает от всех видов вредоносных писем и целевых атак. Его доступность необходимо проверять для выбранной редакции ИКС.

2.9 VPN и защищённый удалённый доступ

VPN позволяет организовать защищённое подключение:

- удалённых сотрудников к сети организации;
- филиалов и отдельных площадок друг к другу;
- администраторов к внутренним ресурсам.

ИКС поддерживает сценарии client-to-site для подключения пользователей и site-to-site для соединения сетей.

Перед подбором необходимо уточнить количество подключений и требования к протоколам.

Встроенные в ИКС VPN не имеют сертификата ФСБ. Если проект требует сертифицированной криптографической защиты, необходимо использовать отдельное средство с соответствующим сертификатом.

2.10 Двухфакторная аутентификация

Двухфакторная аутентификация усиливает защиту удалённого подключения. Для входа пользователю недостаточно знать только пароль — требуется дополнительное подтверждение.

Это снижает риск доступа к корпоративной сети при краже или подборе пароля.

Поддерживаемые способы подтверждения зависят от используемого сценария и версии ИКС.

2.11 Интеграция с AD и ALDPro

ИКС может использовать существующие в организации системы учётных записей.

Интеграция позволяет:

- получать пользователей и группы из каталога;
- применять правила доступа к доменным пользователям;
- использовать централизованную аутентификацию;
- сократить необходимость создания одинаковых учётных записей в разных системах.

Например, правило доступа можно назначить группе «Бухгалтерия» или «Преподаватели», уже созданной в каталоге организации.

Способ интеграции выбирается с учётом используемой службы каталогов и схемы аутентификации. Совместимость конкретной конфигурации следует проверить до поставки.

2.12 Управление пользователями и группами

В ИКС можно создавать пользователей и объединять их в группы, чтобы назначать общие правила.

Для пользователей и групп можно устанавливать:

- разрешённые ресурсы;
- ограничения доступа;
- расписание;
- скорость и объём трафика;
- правила фильтрации.

Групповое управление упрощает администрирование. Вместо настройки каждого сотрудника отдельно правило создаётся один раз и применяется ко всему отделу или группе пользователей.

2.13 Прокси-сервер

Прокси-сервер анализирует запросы от пользователей к интернет-ресурсам. Это позволяет централизованно применять правила доступа, фильтрации и журналирования. Может работать в разных режимах: явный, прозрачный прокси, с полной расшифровкой трафика. ИКС поддерживает сканирование потоковым антивирусом трафика, проходящего через прокси-сервер.

2.14 Мониторинг, отчёты и журналирование

ИКС собирает сведения о работе системы и трафике.

Администратор может просматривать:

- состояние служб и сетевых интерфейсов;
- активность пользователей;
- посещаемые ресурсы;

- использование трафика;
- обнаруженные сетевые события;
- ошибки и действия администраторов.

Отчёты помогают контролировать использование интернета, расследовать инциденты и находить причины сетевых проблем.

2.15 Передача событий в SIEM

ИКС может передавать журналы и события во внешнюю SIEM-систему по протоколу syslog. SIEM собирает данные от ИКС и других средств защиты в одном месте. Это позволяет:

- сопоставлять события из разных источников;
- выявлять связанные подозрительные действия;
- настраивать уведомления;
- проводить расследования;
- централизованно хранить сведения об инцидентах.

Интеграция не означает, что SIEM автоматически распознает все события ИКС. Необходимо проверить формат передаваемых данных и настроить правила их обработки на стороне принимающей системы.

2.16 Отказоустойчивость

ИКС поддерживает отказоустойчивую конфигурацию из двух узлов.

Если основной узел становится недоступен, резервный принимает его функции. Это помогает избежать перерыва в работе интернета и защищаемых сервисов при отказе одного сервера.

Отказоустойчивость следует рассматривать, если через ИКС проходит критичный трафик и простой недопустим.

Для его подбора необходимо привлекать пресейл-инженера.

2.17 Почтовый сервер

В ИКС предусмотрен встроенный почтовый сервер, с помощью которого организация может создавать собственные почтовые домены и ящики.

Он поддерживает основные функции корпоративной почты:

- отправку и получение писем;
- управление почтовыми ящиками;
- адресные книги;
- почтовые квоты;
- защищённую передачу писем;
- DKIM-подпись;
- чёрные и белые списки;
- антивирусную и антиспам-проверку при наличии соответствующих компонентов.

Встроенный сервер может быть полезен организации, которой необходимо объединить сетевой шлюз и почтовые функции в одном решении. Перед его предложением следует оценить количество ящиков, объём почты, требования к хранению и резервному

копированию.

2.18 IP-телефония

ИКС включает виртуальную АТС на базе Asterisk. Она позволяет организовать внутреннюю и внешнюю телефонию:

- создавать телефонные номера;
- настраивать очереди звонков и голосовое меню;
- переводить и перенаправлять вызовы;
- записывать и скачивать разговоры;
- использовать голосовую почту;
- контролировать активные вызовы;
- проводить аудио- и видеоконференции.

Функция может быть полезна небольшой или средней организации, которой требуется собственная IP-телефония.

Перед предложением необходимо уточнить используемого оператора, количество номеров и одновременных разговоров, телефонное оборудование и требования к записи звонков.

2.19 Дополнительные модули и интеграции

Возможности ИКС можно расширять дополнительными коммерческими модулями.

К ним относятся:

Модуль	Назначение
Garnet Web Filter	Категоризация сайтов и создание правил доступа по категориям
Kaspersky Anti-Virus	Потоковая проверка интернет-трафика на вредоносное содержимое
Kaspersky Anti-Spam	Обнаружение нежелательных сообщений в почтовом трафике
Kaspersky Suricata Rules Feed	Обновляемые правила обнаружения сетевых атак для IDS/IPS
«Техподдержка»	Техническая поддержка в первый год с момента покупки ИКС предоставляется бесплатно. Далее продлевается на коммерческой основе.

ИКС также может взаимодействовать с внешними системами и сервисами:

- AD, ALDPro, LDAP — для работы с учётными записями;
- SIEM и syslog-серверами — для передачи событий;
- Zabbix — для контроля состояния системы;
- ICAP-серверами — для внешней обработки поддерживаемого трафика;
- внешними почтовыми системами — в режиме SMTP-релея.

3. Требования регуляторов

3.1 Сертификат и сертифицированные возможности ИКС ФСТЭК

Сертификат ФСТЭК подтверждает, что определённые версия и конфигурация средства защиты прошли испытания и соответствуют указанным в сертификате требованиям безопасности.

ИКС ФСТЭК имеет сертификат соответствия ФСТЭК России № 4832 от 2 августа 2024 года.

В пределах области сертификата продукт может выполнять функции:

- межсетевого экрана типа «А» 4-го класса защиты;
- межсетевого экрана типа «Б» 4-го класса защиты;
- системы обнаружения вторжений сетевого уровня 4-го класса защиты.

ИКС ФСТЭК также соответствует требованиям к средствам защиты информации 4-го уровня доверия.

3.1.1 Что означают сертифицированные функции

Межсетевой экран типа «А» защищает границу информационной системы. Он контролирует обмен данными с внешними сетями, разрешает необходимые соединения, блокирует запрещённые и регистрирует события. Такое применение предусматривает программно-аппаратное исполнение в соответствии с сертифицированной конфигурацией.

Межсетевой экран типа «Б» контролирует обмен данными между сегментами внутри информационной системы. Например, он может разделять рабочие места, серверы, гостевую сеть и технологическое оборудование. В предусмотренных сертификатом случаях возможно программное исполнение.

Система обнаружения вторжений сетевого уровня анализирует трафик и выявляет события, соответствующие признакам известных атак: попытки эксплуатации уязвимостей, сканирование и подозрительные обращения к серверам.

Система обнаружения вторжений решает отдельную задачу и не заменяет антивирус, защиту рабочих станций, контроль действий пользователей и другие меры.

4-й класс защиты и 4-й уровень доверия показывают, по каким требованиям продукт проходил испытания. Партнёру не нужно самостоятельно решать, достаточны ли эти характеристики: это определяется типом системы, её классом или уровнем защищённости, категорией объекта, моделью угроз и проектной документацией.

3.1.2 Область применения

В пределах сертификата ИКС ФСТЭК может применяться:

- в государственных информационных системах до 1-го класса защищённости включительно;
- в информационных системах персональных данных до 1-го уровня защищённости включительно;
- на значимых объектах КИИ до 1-й категории значимости включительно;
- в АСУ ТП до 1-го класса защищённости включительно;

- в информационных системах общего пользования 2-го класса.

Продукт не предназначен для защиты сведений, составляющих государственную тайну.

Сертификат распространяется только на предусмотренные им редакцию, версию, исполнение и конфигурацию. При установке и эксплуатации необходимо соблюдать сертификационную и эксплуатационную документацию.

3.2 Где может применяться ИКС ФСТЭК

Необходимость сертифицированного средства определяется требованиями к конкретной информационной системе, а не только отраслью или формой собственности организации.

Тип системы	Что важно определить	Возможность применения ИКС ФСТЭК
ИСПДн	Уровень защищённости, актуальные угрозы и меры по защите персональных данных	До 1-го уровня включительно, то есть для систем 1–4-го уровней
ГИС	Класс защищённости и требования модели угроз и проекта	До 1-го класса включительно, то есть для ГИС 1–3-го классов
Значимый объект КИИ	Результаты категорирования и категория значимости	До 1-й категории включительно, то есть для объектов 1–3-й категорий
АСУ ТП	Класс защищённости и требования к технологической системе	До 1-го класса включительно
ИСОП	Принадлежность к ИСОП в нормативном смысле и класс защиты	Для ИСОП 2-го класса

3.2.1 Информационные системы персональных данных

ИСПДн — система, в которой персональные данные обрабатываются с использованием средств автоматизации. К таким системам могут относиться кадровая база, CRM, медицинская информационная система и электронный журнал.

Для ИСПДн устанавливается один из четырёх уровней защищённости. Он зависит от категорий и объёма данных, актуальных угроз и других условий. ИКС ФСТЭК может использоваться как один из элементов защиты ИСПДн всех четырёх уровней.

Пример применения: отделить сервер с персональными данными от гостевой сети, разрешить доступ только определённым рабочим местам и контролировать сетевые атаки.

Нормативная основа: Федеральный закон № 152-ФЗ, Постановление Правительства РФ № 1119, приказ ФСТЭК России № 21.

3.2.2 Государственные информационные системы

ГИС создаётся для выполнения полномочий государственных органов и учреждений. Для неё устанавливается 1-й, 2-й или 3-й класс защищённости. ИКС ФСТЭК может применяться в

ГИС всех трёх классов.

Пример применения: контролировать соединения на границе ГИС, ограничить доступ к её серверам и отделить их от рабочих мест, гостевой сети и других сегментов.

Требования к конкретной ГИС определяются её классом, моделью угроз и проектной документацией.

Нормативная основа: Федеральный закон № 149-ФЗ, приказ ФСТЭК России № 17 (приказ ФСТЭК России № 117, вступающему в силу с 01.03.2026).

3.2.3 Значимые объекты КИИ

КИИ включает информационные системы, сети связи и автоматизированные системы управления в установленных законом сферах. Не каждая система субъекта КИИ автоматически является значимым объектом.

Субъект проводит категорирование. Объект, которому присвоена 1-я, 2-я или 3-я категория, признаётся значимым. ИКС ФСТЭК может применяться на объектах всех трёх категорий.

Пример применения: разделить корпоративную и технологическую сеть, разрешить только необходимые соединения и выявлять сетевые атаки.

Нормативная основа: Федеральный закон № 187-ФЗ, приказы ФСТЭК России № 235 и № 239.

3.2.4 Автоматизированные системы управления

АСУ ТП управляют производственными и технологическими процессами. Для их защиты особенно важны сегментация, контроль взаимодействия между корпоративной и технологической сетью и регистрация сетевых событий.

ИКС ФСТЭК может применяться в АСУ ТП до 1-го класса защищённости включительно. Конкретная конфигурация определяется требованиями к объекту и проектной документацией.

Нормативная основа: Приказ ФСТЭК России № 31 (для АСУ ТП, не являющихся значимыми объектами КИИ), приказ ФСТЭК России № 239 (если объект признан значимым)

3.2.5 Информационные системы общего пользования

В нормативном смысле ИСОП — это не любой публичный сайт. К ним относятся определённые федеральные государственные системы, содержащие обязательные для размещения в интернете общедоступные сведения.

Для ИСОП устанавливается 1-й или 2-й класс защиты. ИКС ФСТЭК может применяться в системах 2-го класса.

Пример применения: разместить публичный сервер в отдельном сегменте, контролировать обращения из интернета и ограничить его взаимодействие с внутренними ресурсами.

Нормативная основа: совместный приказ ФСБ России № 416 и ФСТЭК России № 489 от 31 августа 2010 года.

Во всех перечисленных случаях ИКС выполняет сходные сетевые функции: защищает периметр, контролирует трафик, разделяет сегменты, ограничивает соединения,

обнаруживает признаки атак и регистрирует события. Поэтому эти функции не нужно заново перечислять в каждой статье — различаются прежде всего статус системы и допустимая область применения продукта.

3.3 Когда нужны сертифицированные средства защиты

Сертифицированное средство защиты — продукт, соответствие которого установленным требованиям безопасности подтверждено уполномоченным органом.

ФСТЭК России сертифицирует средства технической защиты информации, в том числе межсетевые экраны и системы обнаружения вторжений. Требования к средствам криптографической защиты относятся к компетенции ФСБ России.

Сертифицированное средство может потребоваться:

- когда это прямо предусмотрено законодательством или нормативными требованиями;
- когда его применение установлено для конкретного типа информационной системы;
- когда это указано в модели угроз, проектной или технической документации;
- по решению владельца или оператора системы.

Наличие сертификата само по себе недостаточно. Необходимо проверить:

- назначение и функции средства;
- класс защиты и уровень доверия;
- тип, класс или уровень защищённости информационной системы;
- категорию значимости объекта КИИ;
- версию, исполнение и конфигурацию продукта;
- условия и ограничения сертификата;
- требования к установке, настройке, обновлению и эксплуатации.

3.3.1 Почему одного ИКС недостаточно

Требованиям законодательства и регуляторов должна соответствовать вся система защиты заказчика, а не отдельный продукт.

Помимо ИКС могут потребоваться:

- модель угроз и проектирование системы защиты;
- разграничение прав доступа;
- защита серверов и рабочих мест;
- антивирусная и криптографическая защита;
- резервное копирование и восстановление;
- регистрация и анализ событий;
- реагирование на инциденты;
- организационные документы и регламенты;
- обучение сотрудников;
- контроль настроек, эксплуатации и обновлений.

Поэтому ИКС ФСТЭК следует позиционировать как один из элементов системы защиты, который помогает реализовать предусмотренные проектом меры межсетевого экранирования и обнаружения вторжений.



3.4 ИКС в государственных реестрах

Государственные реестры и сертификат ФСТЭК подтверждают разные характеристики продукта.

Подтверждение	Что оно означает	К чему относится
Реестр российского программного обеспечения	Российское происхождение программы	К программному обеспечению ИКС; реестровая запись № 322
Реестр российской промышленной продукции	Российское происхождение оборудования	Вся линейка ПАК ИКС включена в Реестр российской промышленной продукции
Сертификат ФСТЭК России № 4832	Соответствие установленным требованиям безопасности	К редакции ИКС ФСТЭК и аппаратным платформам, прошедшим сертификацию в качестве ПАК ИКС ФСТЭК.

Если заказчик приобретает программную лицензию, проверяется запись ИКС в Реестре российского ПО.

Если закупается ПАК и к оборудованию предъявляются требования российского происхождения, необходимо отдельно проверить конкретную модель и комплектацию аппаратной платформы в Реестре российской промышленной продукции.

Наличие продукта в реестре не заменяет сертификат ФСТЭК и не гарантирует допуск к любой закупке. Требования извещения, технического задания и актуальность записей необходимо проверять для каждого проекта.

3.5 Памятка партнёру: что можно и нельзя обещать

3.5.1 Что подтверждено

- ИКС включён в Реестр российского программного обеспечения, запись № 322.
- ИКС ФСТЭК имеет сертификат ФСТЭК России № 4832.
- В пределах сертификата продукт может применяться в ГИС до 1-го класса, ИСПДн до 1-го уровня, на значимых объектах КИИ до 1-й категории, в АСУ ТП до 1-го класса и в ИСОП 2-го класса.
- ИКС ФСТЭК сертифицирован как межсетевой экран типов «А» и «Б» и система обнаружения вторжений сетевого уровня.
- Российское происхождение аппаратной части подтверждается отдельно для конкретной модели и комплектации.

3.5.2 Допустимые формулировки

Можно говорить	Почему это корректно
«ИКС ФСТЭК может применяться в пределах области сертификата»	Учитываются назначение и ограничения сертифицированной версии



Можно говорить	Почему это корректно
«ИКС помогает реализовать отдельные технические меры защиты»	Продукт является частью системы защиты
«ИКС обеспечивает межсетевое экранирование и обнаружение сетевых атак в соответствии с сертифицированными функциями»	Обещание ограничено подтверждёнными возможностями
«ИКС включён в Реестр российского ПО»	Это подтверждается реестровой записью № 322
«Выбранная аппаратная платформа включена в промышленный реестр»	Вся линейка ПАК ИКС включена в Реестр российской промышленной продукции
«Конфигурация подбирается с учётом типа системы, модели угроз и проекта»	Требования устанавливаются для конкретного объекта

3.5.3 Недопустимые обещания

Нельзя утверждать:

- «ИКС полностью соответствует 152-ФЗ или 187-ФЗ»;
- «ИКС закрывает все требования ФСТЭК»;
- «После установки ИКС система автоматически станет защищённой»;
- «С ИКС заказчик гарантированно пройдёт проверку или аттестацию»;
- «ИКС исключает утечки, атаки и инциденты»;
- «Обычная редакция NGFW ИКС равнозначна ИКС ФСТЭК»;
- «Любая версия, конфигурация или аппаратная платформа входит в область сертификата»;
- «ИКС подходит для любой ГИС, ИСПДн или КИИ без анализа требований»;
- «Сертификат ФСТЭК подтверждает выполнение требований ФСБ»;
- «Наличие ИКС в реестрах автоматически обеспечивает допуск к закупке».

3.5.4 Как заменить опасные формулировки

Вместо «ИКС соответствует 152-ФЗ»: ИКС ФСТЭК может использоваться для реализации отдельных мер защиты персональных данных, предусмотренных для конкретной ИСПДн.

Вместо «ИКС закрывает требования по КИИ»: ИКС ФСТЭК может применяться как один из элементов системы безопасности значимого объекта КИИ в пределах области сертификата.

Вместо «с ИКС заказчик пройдёт проверку»: ИКС помогает выполнить предусмотренные проектом технические меры, но результат проверки зависит от всей системы защиты и её эксплуатации.

Вместо «это полностью российский ПАК»: Программное обеспечение ИКС включено в Реестр российского ПО. Статус аппаратной части подтверждается отдельно для выбранной модели и комплектации.

3.5.5 Что уточнить перед предложением

1. Какую информационную систему требуется защитить.
2. Относится ли она к ГИС, ИСПДн, КИИ, АСУ ТП или ИСОП.
3. Какой класс, уровень защищённости или категория значимости установлены.
4. Какие угрозы признаны актуальными.
5. Какие меры предусмотрены моделью угроз и проектной документацией.
6. Требуется ли сертифицированный межсетевой экран или система обнаружения вторжений.
7. Нужны ли российское ПО и оборудование из промышленного реестра.
8. Какая редакция, версия, конфигурация и производительность необходимы.
9. Есть ли подходящая платформа или нужен готовый ПАК.

Если заказчик не может определить тип системы, её класс, уровень, категорию или необходимые меры, партнёру нельзя самостоятельно обещать соответствие. К подбору необходимо привлечь технического специалиста или специалиста по информационной безопасности.

3.5.6 Главное правило

Партнёр продаёт подтверждённые возможности ИКС, а не гарантированное соответствие всей организации законодательству.

Корректная итоговая формулировка:

ИКС ФСТЭК — сертифицированное средство защиты, которое может применяться в пределах области сертификата и помогать реализовать предусмотренные проектом технические меры. Соответствие требованиям определяется для всей информационной системы заказчика.

4. Целевые заказчики и сценарии применения

4.1 Портрет целевого заказчика

Целевой заказчик ИКС — организация, которой требуется защитить сетевой периметр, контролировать трафик, разграничивать доступ между сегментами сети, фильтровать интернет-ресурсы и регистрировать события безопасности.

Наиболее типичный заказчик имеет:

- от 30 до 1500 пользователей;
- серверы, информационные системы или облачные сервисы;
- постоянное подключение к интернету;
- системного администратора или ИТ/ИБ-службу;
- потребность в российском межсетевом экране;
- требования к контролю доступа и регистрации событий;
- бюджет на внедрение и сопровождение.

ИКС особенно актуален для организаций, которым нужен функциональный продукт без избыточной сложности эксплуатации.

4.1.1 Основные причины приобретения

Заказчики рассматривают ИКС, когда необходимо:

- заменить зарубежный или больше не поддерживаемый межсетевой экран;
- защитить сеть от несанкционированных подключений и сетевых атак;
- разделить пользовательские, серверные, гостевые и другие сегменты;
- ограничить посещение нежелательных интернет-ресурсов;
- контролировать использование интернет-канала;
- получать отчёты о работе пользователей в интернете;
- регистрировать и передавать события безопасности;
- реализовать предусмотренные проектом меры защиты информации;
- перейти на российское программное обеспечение;
- приобрести межсетевой экран вместе с аппаратной платформой.

Если организации требуется VPN для удалённой работы или связи офисов, необходимо сначала определить, будет ли по этому соединению передаваться информация из регулируемой системы.

VPN, встроенные в ИКС, не имеют сертификата ФСБ. Поэтому их нельзя предлагать как сертифицированное средство криптографической защиты. В регулируемых системах защищённые каналы связи должны организовываться с помощью отдельного средства, имеющего требуемый сертификат ФСБ.

4.2 Государственные и муниципальные организации

К этой группе относятся администрации, министерства, департаменты, комитеты, казённые и бюджетные учреждения, МФЦ, архивы, фонды и другие государственные и муниципальные организации.

Такие заказчики могут работать с персональными данными, служебной информацией и

государственными информационными системами. Для них особенно важны наличие сертификата ФСТЭК, российское происхождение продукта и соответствие средства защиты проектной документации.

4.2.1 Типовые задачи

ИКС ФСТЭК может применяться для:

- защиты подключения учреждения к интернету;
- фильтрации входящего и исходящего трафика;
- разграничения доступа сотрудников и подразделений;
- отделения серверов от пользовательской сети;
- защиты информационных систем от неразрешённых сетевых подключений;
- обнаружения признаков сетевых атак;
- регистрации событий безопасности;
- передачи журналов во внешнюю систему мониторинга;
- ограничения доступа к нежелательным интернет-ресурсам;
- замены зарубежного межсетевого экрана;
- Соответствия требованиям регуляторов и реализации отдельных мер защиты ГИС и ИСПДн.

4.2.2 Пример заказчика

Районная администрация эксплуатирует ГИС и ИСПДн. Серверы информационных систем размещены в отдельном сегменте, однако правила доступа между серверной и пользовательской сетями устарели, а события безопасности не передаются в систему мониторинга.

ИКС ФСТЭК можно разместить на границе защищаемой сети или между её сегментами. Он будет контролировать сетевые соединения, разрешать только необходимые взаимодействия и регистрировать события безопасности.

Если администрации требуется связать несколько зданий или предоставить удалённый доступ к регулируемой системе, для создания защищённых каналов необходимо использовать отдельное средство с требуемым сертификатом ФСБ. Встроенный VPN ИКС для этого сценария не подходит.

4.2.3 Что спросить у заказчика

1. Какую информационную систему необходимо защитить?
2. Относится ли она к ГИС или ИСПДн?
3. Определены ли класс или уровень защищённости?
4. Требуется ли сертификат ФСТЭК?
5. Какие функции межсетевого экрана предусмотрены моделью угроз и техническим заданием?
6. Какие сетевые сегменты и информационные ресурсы необходимо разделить?
7. Нужна ли передача событий в SIEM или другую систему мониторинга?
8. Требуется ли защищённые соединения между зданиями или для удалённого доступа? Если да, предусмотрено ли отдельное сертифицированное ФСБ средство?
9. Нужен программный продукт или готовый ПАК?

Нельзя обещать, что приобретение ИКС само по себе обеспечит выполнение всех требований законодательства или гарантирует прохождение аттестации.

4.3 Образовательные учреждения

К этой группе относятся детские сады, школы, колледжи, техникумы, университеты, учреждения дополнительного образования, библиотеки, учебные центры и детские организации.

В образовательной сети одновременно работают администрация, преподаватели, обучающиеся и гости. Для разных групп должны действовать разные правила доступа.

4.3.1 Типовые задачи

ИКС может использоваться для:

- разделения административной, учебной и гостевой сетей;
- ограничения доступа обучающихся к нежелательным ресурсам;
- контроля использования интернет-канала;
- применения разных правил для сотрудников и обучающихся;
- защиты серверов и внутренних информационных систем;
- обнаружения сетевых атак;
- регистрации действий пользователей и сетевых событий;
- замены зарубежного межсетевого экрана.

Если защищаемая сеть относится к ИСПДн или ГИС и в проекте требуется сертифицированный межсетевой экран, следует рассматривать ИКС ФСТЭК.

4.3.2 Пример заказчика

В колледже одной сетью пользуются администрация, преподаватели и студенты. Учащиеся могут обращаться к ресурсам административного сегмента, а единые правила фильтрации не учитывают различия между группами пользователей.

ИКС позволяет разделить административную, учебную и гостевую сети, настроить разные правила доступа и ограничить посещение нежелательных ресурсов. Для категоризации сайтов отдельно рассматривается модуль Garnet Web Filter.

4.3.3 Что спросить у заказчика

1. Сколько сотрудников и обучающихся одновременно используют сеть?
2. Есть ли отдельные сети для администрации, учащихся и гостей?
3. Какие внутренние системы и серверы необходимо защитить?
4. Какие категории интернет-ресурсов требуется ограничивать?
5. Нужно ли применять разные правила для учеников и преподавателей?
6. Требуется ли идентификация пользователей через каталог учётных записей?
7. Обрабатываются ли в системе персональные данные?
8. Относится ли защищаемая система к ГИС или ИСПДн?
9. Нужен ли сертифицированный межсетевой экран?

Перспективный заказчик — учреждение, которое обновляет сеть, внедряет гостевой Wi-Fi, разделяет пользователей, сталкивается с перегрузкой канала или переходит от ручной блокировки сайтов к централизованному контролю.

4.4 Медицинские организации

К медицинским заказчикам относятся больницы, поликлиники, диагностические центры, лаборатории, стоматологии, медицинские информационно-аналитические центры и частные клиники.

Медицинские организации обрабатывают персональные данные и сведения о здоровье, а также подключаются к единой государственной системе здравоохранения. При этом требования к защите определяются отдельно для каждой информационной системы.

4.4.1 Типовые задачи

ИКС ФСТЭК может применяться для:

- защиты сетевого периметра;
- сегментации административной, медицинской и гостевой инфраструктуры;
- ограничения доступа к медицинским серверам;
- контроля сетевых соединений;
- отделения медицинского оборудования от пользовательских компьютеров;
- обнаружения признаков атак;
- регистрации событий безопасности;
- передачи событий во внешнюю систему мониторинга;
- фильтрации интернет-доступа;
- замены зарубежного межсетевого экрана;
- Соответствия требованиям регуляторов и реализации отдельных мер защиты ИСПДн, ГИС или объекта КИИ.

4.4.2 Пример заказчика

В поликлинике медицинская информационная система, рабочие места сотрудников, медицинское оборудование и гостевой Wi-Fi находятся в неразделённых сегментах. Необходимо исключить прямой доступ посетителей и обычных пользовательских компьютеров к медицинским серверам.

ИКС ФСТЭК можно использовать для сегментации сети, контроля разрешённых соединений, обнаружения подозрительной активности и регистрации событий безопасности.

Если филиалам или удалённым кабинетам требуется доступ к единой государственной системе здравоохранения, защищённые каналы должны создаваться отдельным средством с необходимым сертификатом ФСБ. VPN ИКС не следует включать в такой сценарий.

4.4.3 Что спросить у заказчика

1. Какие информационные системы необходимо защитить?
2. Какие персональные данные в них обрабатываются?
3. Определён ли уровень защищённости ИСПДн?
4. Является ли информационная система государственной?
5. Относится ли организация или система к КИИ?
6. Требуется ли сертификат ФСТЭК?
7. Нужно ли отделить медицинское оборудование от пользовательской сети?
8. Требуется ли изолировать гостевой Wi-Fi?
9. Какие сервисы должны быть доступны непрерывно?

10. Есть ли требования к сертифицированной криптографии?

Корректно говорить, что ИКС ФСТЭК может применяться для реализации отдельных технических мер защиты в пределах сертификата и проектных требований. Нельзя утверждать, что продукт самостоятельно обеспечивает соответствие всем требованиям регуляторов.

4.5 Промышленные предприятия

К этой группе относятся заводы, производственные компании, добывающие предприятия, энергетические организации, складские комплексы и другие предприятия с производственной инфраструктурой.

Главная особенность таких заказчиков — одновременное существование корпоративных и технологических сетей. Несанкционированный доступ к производственному сегменту может повлиять на непрерывность технологического процесса.

4.5.1 Типовые задачи

ИКС может применяться для:

- разделения офисной и производственной сетей;
- контроля соединений между сетевыми сегментами;
- ограничения доступа подрядчиков;
- защиты внешнего периметра;
- обнаружения подозрительной сетевой активности;
- регистрации событий безопасности;
- резервирования межсетевого экрана;
- передачи событий в SIEM;
- импортозамещения зарубежного решения;
- соответствия требованиям регуляторов и реализации отдельных мер защиты КИИ или АСУ ТП.

4.5.2 Пример заказчика

На предприятии производственный сервер получает данные из технологического сегмента и передаёт отчёты в корпоративную систему. При этом офисные компьютеры имеют избыточный доступ к производственной сети.

ИКС можно установить между корпоративным и технологическим сегментами и разрешить только заранее определённые соединения. Если объект относится к КИИ или АСУ ТП и требуется сертифицированное средство, возможность применения ИКС ФСТЭК проверяется по проектной документации и области действия сертификата.

Удалённый доступ подрядчиков и соединение производственных площадок не следует строить на VPN ИКС, если для этих соединений требуется сертифицированная криптографическая защита. В таком случае применяется отдельное средство с необходимым сертификатом ФСБ.

4.5.3 Что спросить у заказчика

1. Нужно защитить корпоративную или технологическую сеть?

2. Какие сегменты необходимо разделить?
3. Какие соединения между сегментами должны быть разрешены?
4. Какие сетевые протоколы используются?
5. Является ли объект значимым объектом КИИ?
6. Относится ли система к АСУ ТП?
7. Требуется ли сертифицированное решение?
8. Какова критичность простоя?
9. Нужна ли отказоустойчивая конфигурация?
10. Какова фактическая пропускная способность?
11. Требуется ли сертифицированная криптографическая защита каналов?

Если речь идёт о специализированных промышленных протоколах, экстремальных условиях эксплуатации или высокоскоростной инфраструктуре, проект требует отдельной технической проработки.

4.6 Малый и средний бизнес

К этой группе относятся торговые, сервисные, строительные, логистические, проектные и другие коммерческие организации. Обычно у них нет большой службы информационной безопасности, поэтому одно решение должно закрывать несколько повседневных сетевых задач.

4.6.1 Типовые задачи

ИКС может использоваться для:

- защиты офисной сети;
- управления доступом сотрудников в интернет;
- ограничения нежелательных ресурсов;
- контроля использования интернет-канала;
- подготовки отчётов;
- разделения рабочей, серверной и гостевой сетей;
- обнаружения сетевых атак;
- публикации внутренних сервисов;
- замены нескольких отдельных решений одним продуктом;
- перехода с зарубежного межсетевого экрана.

Для обычной корпоративной сети, в которой отсутствует требование использовать сертифицированную криптографическую защиту, встроенные VPN ИКС могут применяться для удалённого доступа и соединения офисов.

Если через соединение передаётся информация регулируемой системы, необходимо проверить требования к криптографической защите. При необходимости сертифицированной криптографии используется отдельное средство с сертификатом ФСБ.

4.6.2 Пример заказчика

В компании работают 80 сотрудников. Серверы, рабочие места и гостевой Wi-Fi находятся в общей сети, сотрудники бесконтрольно используют интернет, а действующий зарубежный межсетевой экран больше не продлевается.

ИКС позволяет разделить сеть, настроить правила интернет-доступа, контролировать трафик и заменить зарубежное решение российским продуктом.

4.6.3 Что спросить у заказчика

1. Сколько пользователей и устройств в организации?
2. Какова скорость интернет-канала?
3. Какие сетевые сегменты необходимо разделить?
4. Какие сервисы опубликованы в интернете?
5. Требуется ли ограничивать сайты и приложения?
6. Нужны ли отчёты о действиях пользователей?
7. Какое решение используется сейчас?
8. Есть ли собственный системный администратор?
9. Требуются ли удалённые подключения или связь между офисами?
10. Передаются ли через такие соединения данные регулируемых систем?
11. Требуется ли сертифицированная криптографическая защита каналов?
12. Планируется ли рост компании?

4.7 Организации с филиальной структурой

Филиальная структура встречается в торговых сетях, медицинских и образовательных организациях, органах власти, промышленных предприятиях и сервисных компаниях.

Однако наличие филиалов само по себе не означает, что для связи между ними можно использовать VPN ИКС. Сначала необходимо определить характер передаваемой информации и требования к криптографической защите.

4.7.1 Сценарий без обязательной сертифицированной криптографии

Если коммерческая организация объединяет обычные корпоративные сети и не обязана применять сертифицированное средство криптографической защиты, VPN ИКС может использоваться для:

- создания туннелей между площадками;
- подключения филиалов к корпоративным сервисам;
- удалённого доступа сотрудников;
- ограничения взаимодействия между филиалами;
- защиты локального выхода каждого филиала в интернет.

4.7.2 Пример заказчика

У торговой компании есть центральный офис, склад и пять магазинов. В филиалах работают кассовые системы, ведётся складской учёт и используются общие корпоративные сервисы. Передаваемая между площадками информация не относится к регулируемым информационным системам, а требования к применению сертифицированной криптографии отсутствуют.

На каждой площадке можно установить ИКС для защиты локальной сети и контроля интернет-доступа, а встроенный VPN использовать для создания защищённых туннелей между магазинами, складом и центральным офисом. Через эти соединения сотрудники смогут обращаться к корпоративным сервисам, системе складского учёта и другим внутренним

ресурсам.

4.7.3 Сценарий регулируемой системы

Если между площадками передаются данные ГИС, ИСПДн, КИИ, АСУ ТП или другой регулируемой системы и проект требует сертифицированной криптографической защиты, VPN ИКС для организации такого канала не применяется.

В этом случае:

- ИКС ФСТЭК выполняет функции межсетевого экрана;
- отдельное сертифицированное ФСБ средство обеспечивает криптографическую защиту канала;
- схема совместного применения определяется проектной документацией.

4.7.4 Пример заказчика

У медицинской организации есть головная площадка и несколько филиалов. На каждой площадке необходимо защитить локальную сеть, разделить рабочие места, медицинское оборудование и гостевой Wi-Fi, а также контролировать доступ к интернету.

ИКС ФСТЭК может использоваться на площадках как межсетевой экран. Каналы связи с центральной медицинской системой должны быть организованы отдельным средством с необходимым сертификатом ФСБ.

4.7.5 Что спросить у заказчика

1. Сколько площадок необходимо защитить?
2. Какие информационные системы используются в филиалах?
3. Какие данные передаются между площадками?
4. Относятся ли эти системы к ГИС, ИСПДн, КИИ или АСУ ТП?
5. Требуется ли сертифицированная криптографическая защита каналов?
6. Какое средство используется для защиты межфилиальных соединений сейчас?
7. Предусмотрено ли отдельное средство с сертификатом ФСБ?
8. Где должен устанавливаться межсетевой экран?
9. Нужен ли каждому филиалу собственный выход в интернет?
10. Какие сегменты необходимо разделить на каждой площадке?
11. Требуются ли единые правила защиты для всех филиалов?
12. Кто будет администрировать решения?

4.8 Признаки потенциальной потребности в ИКС

Заказчик не всегда формулирует потребность как покупку межсетевого экрана. Он может говорить о незащищённой сети, отсутствии контроля интернет-доступа, импортозамещении или подготовке к аттестации.

4.8.1 Организационные признаки

Потребность возможна, если заказчик:

- открывает новый офис или производственную площадку;
- увеличивает количество сотрудников;
- внедряет новую информационную систему;
- разделяет общую инфраструктуру на отдельные сегменты;

- создаёт ИТ- или ИБ-службу;
- готовится к проверке или аттестации;
- разрабатывает модель угроз и систему защиты;
- переходит на российское программное обеспечение.

4.8.2 Технические признаки

ИКС стоит включить в рассмотрение, если:

- на границе сети используется обычный маршрутизатор/роутер/«самописное» решение;
- правила доступа настроены бессистемно;
- рабочая, серверная и гостевая сети не разделены;
- серверы доступны из пользовательского сегмента без ограничений;
- нельзя определить, кто и как использует интернет;
- интернет-канал регулярно перегружен;
- события безопасности не регистрируются;
- действующее решение не справляется с нагрузкой;
- требуется контролировать соединения между сегментами;
- необходимо заменить зарубежный межсетевой экран.

4.9 Как позиционировать ИКС для заказчика

Позиционирование — это краткое объяснение того, для каких задач подходит ИКС и какую пользу он приносит конкретному заказчику. В разговоре следует начинать не с перечня функций, а с задач организации, рисков и требований к будущему решению.

4.9.1 Основное позиционирование

ИКС — российский NGFW для небольших и средних организаций, которым необходимо защищать сетевой периметр, контролировать трафик и доступ пользователей, обнаруживать сетевые атаки и управлять основными сетевыми функциями через единый веб-интерфейс.

Продукт подходит организациям, которым требуется функциональное решение без развёртывания избыточно сложной инфраструктуры. ИКС можно поставить в виде программной лицензии или программно-аппаратного комплекса. Для проектов, в которых предусмотрено применение сертифицированного межсетевого экрана, существует редакция ИКС ФСТЭК.

ИКС не следует представлять как универсальное решение для любой инфраструктуры. Соответствие продукта требованиям заказчика, необходимую производительность и состав поставки определяют после сбора исходных данных.

4.9.2 Когда стоит предлагать ИКС

ИКС следует рассматривать, если заказчику необходимо:

- защитить сетевой периметр организации;
- контролировать доступ пользователей, устройств или сетевых сегментов;
- ограничивать доступ к интернет-ресурсам и приложениям;
- обнаруживать признаки сетевых атак;
- вести журналы событий и формировать отчёты;
- заменить зарубежный межсетевой экран российским продуктом;

- объединить основные сетевые функции и средства контроля в одном решении;
- приобрести программное решение для существующего сервера или виртуальной среды;
- получить готовый программно-аппаратный комплекс;
- применить сертифицированный ФСТЭК межсетевой экран, если это предусмотрено проектом защиты;
- организовать сопровождение решения с помощью российской технической поддержки.

Перед предложением продукта необходимо убедиться, что ИКС соответствует масштабу сети, нагрузке, обязательным функциям, интеграциям и требованиям к сертификации.

4.9.3 Ценность для разных участников выбора

Участник	Что для него важно	Какую ценность доносить
Руководитель	Стабильность работы, снижение рисков, бюджет, импортозамещение, ответственность поставщика	ИКС помогает защитить корпоративную сеть, контролировать использование интернет-доступа и объединить несколько функций в одном российском решении. Можно выбрать программную поставку или ПАК с учётом инфраструктуры и бюджета
ИТ-специалист	Удобство управления, совместимость, внедрение, сопровождение, нагрузка на команду	Основные сетевые функции доступны через единый веб-интерфейс. ИКС можно развернуть на совместимом сервере, в виртуальной среде или приобрести вместе с оборудованием. До покупки решение можно проверить на пилоте
Специалист по ИБ	Контроль трафика, сегментация, обнаружение атак, журналирование, интеграции, выполнение требований проекта защиты	ИКС позволяет устанавливать правила доступа, контролировать взаимодействие сетевых сегментов, использовать IDS/IPS, вести журналы и передавать события во внешнюю SIEM. Для регулируемых систем предусмотрена редакция ИКС ФСТЭК

Менеджеру следует менять акцент в зависимости от собеседника. Руководителю необходимо показывать влияние решения на работу организации, ИТ-специалисту — удобство внедрения и эксплуатации, специалисту по ИБ — возможности контроля и соответствие требованиям проекта защиты.

4.10 Нецелевые заказчики и проекты

ИКС не следует предлагать любому заказчику, которому требуется «что-нибудь для безопасности». Сначала необходимо убедиться, что задачи соответствуют назначению и подтверждённым возможностям продукта.

4.10.1 Проекты, которые обычно не являются целевыми

ИКС не заменяет:

- антивирус для рабочих станций;
- DLP-систему;
- SIEM;
- специализированный WAF;
- облачную защиту от DDoS;
- систему резервного копирования;
- средство управления мобильными устройствами;
- сертифицированное средство криптографической защиты информации.

VPN ИКС не имеет сертификата ФСБ. Поэтому ИКС нельзя предлагать как замену сертифицированному криптошлюзу или как единственное решение для создания защищённых каналов в регулируемых системах.

4.10.2 Проекты, требующие отдельной проверки

Дополнительная техническая проработка необходима, если заказчику нужны:

- характеристики, превышающие возможности доступных платформ;
- специализированные промышленные интерфейсы или протоколы;
- работа в нестандартных физических условиях;
- функции, отсутствующие в текущей версии продукта;
- обязательная совместимость с конкретной системой;
- централизованное управление большим числом узлов;
- размещение решения в нестандартной сетевой схеме.

4.10.3 Что нельзя обещать

Нельзя заявлять, что ИКС:

- гарантированно предотвратит все атаки;
- полностью исключит утечки информации;
- самостоятельно обеспечит соответствие законодательству;
- гарантирует прохождение проверки или аттестации;
- заменит все средства информационной безопасности;
- является сертифицированным ФСБ средством криптографической защиты;
- подходит для регулируемой системы без проверки сертификата и проектных требований.

5. Подбор решения

Подбор ИКС начинается не с выбора лицензии или оборудования, а с изучения задач и инфраструктуры заказчика. Ошибка на этом этапе может привести к нехватке производительности, избыточной стоимости или поставке решения, которое не соответствует требованиям проекта.

5.1 Сведения, необходимые для подбора

Перед подготовкой спецификации необходимо выяснить:

1. Для какой сети или информационной системы приобретается ИКС.
2. Требуется ли сертификат ФСТЭК.
3. Сколько пользователей и устройств будет работать через ИКС.
4. Какова скорость интернет-канала.
5. Какие функции будут использоваться.
6. Есть ли у заказчика сервер или виртуальная инфраструктура.
7. Нужна ли поставка готового программно-аппаратного комплекса.
8. Требуется ли резервирование.
9. Планируется ли увеличение нагрузки.
10. Есть ли специальные требования к оборудованию и сетевой схеме.

Эти сведения фиксируются в опросном листе (шаблон находится в разделе Коммерческие и маркетинговые материалы). Если заказчик не может предоставить точные параметры, необходимо запросить схему сети или привлечь пресейл-инженера вендора.

5.2 Определение количества пользователей

Лицензия ИКС подбирается по количеству пользователей, которым разрешена работа через продукт.

При расчёте необходимо учитывать не только сотрудников, но и другие учётные записи, которые будут использовать ИКС. Например:

- преподавателей и учащихся;
- сотрудников филиалов;
- временных работников;
- подрядчиков;
- общие и служебные учётные записи;
- планируемое расширение штата.

Количество пользователей не всегда совпадает с числом компьютеров или одновременных подключений.

5.2.1 Как выполнить расчёт

1. Определить текущее количество пользователей.
2. Добавить пользователей, которые подключатся после внедрения.
3. Проверить наличие временных и служебных учётных записей.
4. Учесть планируемый рост организации.
5. Выбрать ближайший подходящий вариант лицензии.

Не следует подбирать лицензию только по текущему числу активных сотрудников, если в ближайшее время ожидается расширение.

5.3 Выбор редакции и варианта поставки

5.3.1 NGFW ИКС или ИКС ФСТЭК

NGFW ИКС подходит для корпоративных сетей, в которых не требуется применение сертифицированного ФСТЭК межсетевого экрана.

ИКС ФСТЭК рассматривается, если средство защиты используется в ГИС, ИСПДн, КИИ, АСУ ТП или другой регулируемой системе и необходимость сертификата установлена проектными документами.

5.3.2 Программная лицензия или ПАК

Программная лицензия подходит, если у заказчика есть совместимый сервер или виртуальная инфраструктура. Перед поставкой необходимо проверить ресурсы, сетевые интерфейсы и совместимость оборудования.

ПАК следует предлагать, если заказчику:

- требуется готовое решение;
- не подходит существующий сервер;
- требуется сертифицированный программно-аппаратный комплекс.

Вариант поставки не изменяет назначение продукта. Он определяет, на каком оборудовании будет работать ИКС.

5.4 Подбор производительности, модулей и отказоустойчивости

5.4.1 Производительность

Аппаратная платформа подбирается не только по количеству пользователей. На нагрузку также влияют:

- скорость интернет-канала;
- количество одновременных соединений;
- объём трафика между сегментами;
- использование IDS/IPS;
- антивирусная проверка;
- фильтрация и анализ трафика;
- количество правил;
- ведение журналов и отчётов;
- резерв производительности на рост.

Нельзя обещать требуемую производительность только на основании числа сотрудников. Для сложных конфигураций необходим технический расчёт.

5.4.2 Дополнительные коммерческие модули

Потребность заказчика	Что рассмотреть	Присутствует в версии
Категоризация интернет-ресурсов	Garnet Web Filter	NGFW ИКС
Проверка интернет-трафика на вредоносное содержимое	Kaspersky Anti-Virus	NGFW ИКС
Защита почтового сервера от нежелательных сообщений	Kaspersky Anti-Spam	NGFW ИКС
Расширение правил обнаружения сетевых атак	Kaspersky Suricata Rules Feed	NGFW ИКС/ ИКС ФСТЭК

5.4.3 Отказоустойчивая конфигурация

Кластер рассматривается, если остановка межсетевого экрана приведёт к недоступности критичных сервисов или прекращению работы организации.

Отказоустойчивая конфигурация обычно требуется, когда:

- через ИКС проходит весь доступ организации в интернет;
- решение защищает критичные сетевые сегменты;
- простой недопустим;
- отсутствует резервный маршрут;
- требования к доступности установлены техническим заданием.

Для кластера предусматриваются два сопоставимых узла. Также необходимо проверить сетевую схему, количество интерфейсов, соединение между узлами и порядок переключения.

Кластер защищает от отказа одного узла, но не заменяет резервирование электропитания, каналов связи и другого сетевого оборудования.

5.5 Когда привлекать пресейл-инженера вендора

Менеджер может самостоятельно подготовить типовую спецификацию, если понятны количество пользователей, редакция, вариант поставки и необходимые модули.

Пресейл-инженера необходимо привлечь, если:

- заказчик не может описать сетевую схему;
- требуется расчёт производительности;
- используются каналы высокой скорости;
- планируется кластер;
- необходимо подобрать сервер;
- в проекте несколько площадок или сложная сегментация;
- требуется интеграция с другими средствами защиты;
- необходимо проверить совместимость;
- проект относится к ГИС, ИСПДн, КИИ или АСУ ТП;
- техническое задание содержит неоднозначные требования;

- заказчик запрашивает функцию, наличие которой не подтверждено;
- планируется пилотное тестирование;
- цена ошибки при подборе высока.

Пресейл-инженеру необходимо передать заполненный опросный лист, схему сети, требования заказчика и предварительную спецификацию.

5.5.1 Итоговый порядок подбора

1. Определить задачи и тип защищаемой системы.
2. Уточнить требования к сертификации.
3. Рассчитать количество пользователей.
4. Выбрать редакцию ИКС.
5. Определить вариант поставки.
6. Рассчитать необходимую производительность.
7. Добавить нужные модули.
8. Определить необходимость кластера.
9. Проверить возможность роста.
10. При необходимости согласовать решение с пресейл-инженером.
11. Сформировать итоговую спецификацию для заказчика.

5.6 Проекты от 100 пользователей

Для проектов от 100 пользователей партнёр может привлечь пресейл-инженера вендора, провести ВКС с заказчиком и организовать тестирование ИКС. До подключения специалиста необходимо собрать базовые сведения: задачу, количество пользователей, скорость каналов, требуемые функции, схему сети и требования к сертификации.

Эти возможности помогают партнёру увереннее вести проект, подтвердить техническое соответствие и снизить риск ошибки при подборе. ВКС и тестирование не заменяют квалификацию проекта: у встречи должна быть понятная цель, а у пилота — согласованные сценарии и критерии результата.

6. Лицензирование

ИКС лицензируется по количеству включённых пользователей. Коммерческая лицензия действует бессрочно. Модуль «Техподдержка» предоставляется бесплатно на первый год, а со второго года приобретается ежегодно. Минимальная коммерческая лицензия начинается с 30 пользователей. Максимальная рассчитана на 1500 пользователей. Проекты с числом пользователей свыше 1500 необходимо обсуждать с вендором.

6.1 Принцип лицензирования

Лицензионный лимит определяется количеством включённых пользователей ИКС.

Пользователем может быть:

- учётная запись сотрудника;
- учётная запись учащегося или подрядчика;
- общая или служебная учётная запись;
- отдельный компьютер, если доступ организован без персональной учётной записи.

Отключённые пользователи лицензию не занимают.

Количество пользователей не всегда совпадает с числом сотрудников, устройств или одновременных подключений. Расчёт зависит от того, как в ИКС организованы учётные записи и доступ.

Перед подбором лицензии необходимо определить:

1. Сколько пользователей будет включено в ИКС.
2. Как организована их авторизация.
3. Есть ли общие и служебные учётные записи.
4. Планируется ли увеличение количества пользователей.

Если схема доступа заказчика неясна, расчёт следует согласовать с техническим специалистом.

6.2 Виды лицензий

6.2.1 Пробная лицензия (Trial)

Предназначена для тестирования ИКС перед покупкой. Она позволяет проверить функции продукта, совместимость с инфраструктурой и производительность.

Срок тестирования 35 дней с момента установки ИКС. При необходимости можно согласовать с вендором более длительный период тестирования.

При переходе на коммерческую лицензию настройки, выполненные во время тестирования, можно сохранить.

6.2.2 Коммерческая лицензия

Коммерческая лицензия приобретается на определённое количество пользователей. Право использования лицензии предоставляется бессрочно.

В первый год после покупки бесплатно предоставляется модуль «Техподдержка». Со второго года его необходимо приобретать ежегодно.

Дополнительно могут приобретаться Garnet Web Filter и модули Kaspersky.

Состав поставки, количество пользователей и список модулей указываются в спецификации.

6.2.3 ИКС Lite

ИКС Lite — бесплатная версия для небольших сетей. Она поддерживает:

- до 9 пользователей, включая администратора;
- до 9 почтовых ящиков;
- до 9 Jabber-аккаунтов;
- до 9 телефонных номеров;
- доступ к серверу обновлений.

Техническая поддержка ИКС Lite не предоставляется. Расширение ИКС Lite не предусмотрено. Если требуется 10 и более пользователей, необходимо приобрести минимальную коммерческую лицензию на 30 пользователей.

6.3 Техподдержка и дополнительные модули

6.3.1 Модуль «Техподдержка»

Модуль «Техподдержка» помогает поддерживать ИКС в актуальном и безопасном состоянии.

Он предоставляет доступ к:

- новым версиям ИКС;
- обновлениям безопасности;
- исправлениям выявленных ошибок и уязвимостей;
- консультациям технических специалистов;
- удалённому подключению инженера при необходимости.

Модуль предоставляется бесплатно на первый год с момента покупки ИКС. Со второго года он приобретается ежегодно.

Основная лицензия продолжает работать и без действующей техподдержки. Однако клиент не получает новые версии, актуальные исправления и помощь технических специалистов. Со временем это увеличивает риски эксплуатации устаревшей версии и усложняет устранение технических проблем. Поэтому продление следует предлагать не как формальную дополнительную услугу, а как необходимое условие безопасной и стабильной эксплуатации ИКС.

Менеджеру рекомендуется:

1. Заранее контролировать дату окончания бесплатного периода.
2. Объяснить клиенту, какие возможности предоставляет модуль.
3. Направить предложение на продление до окончания его действия.
4. Не допускать перерыва между бесплатным и платным периодами.
5. Ежегодно включать продление в работу по удержанию клиента.



6.3.2 Дополнительные модули

Модуль	Назначение	Наличие в версии	Активация модуля
Garnet Web Filter	Категоризация и фильтрация сайтов	NGFW ИКС	На стороне вендора
Kaspersky Anti-Virus	Проверка интернет-трафика	NGFW ИКС	Клиенту предоставляется ссылка для получения ключа
Kaspersky Anti-Spam	Фильтрация SMTP-трафика	NGFW ИКС	Клиенту предоставляется ссылка для получения ключа
Kaspersky Suricata Rules Feed	Обновляемые правила обнаружения атак	NGFW ИКС и ИКС ФСТЭК	На стороне вендора
Модуль «Техподдержка»	Обновления и помощь специалистов	NGFW ИКС и ИКС ФСТЭК	На стороне вендора

Все коммерческие модули лицензируются по количеству пользователей.

Каждый модуль можно бесплатно протестировать в течение 30 дней перед приобретением.

Для активации модулей Kaspersky Anti-Virus и Kaspersky Anti-Spam используются специальные ключи, предназначенные для ИКС. Обычные лицензии продуктов Kaspersky для их активации не подходят.

6.4 Срок действия лицензии и модулей

Коммерческая лицензия ИКС действует бессрочно.

Модуль «Техподдержка»:

- предоставляется бесплатно на первый год после покупки ИКС;
- со второго года приобретается на платной основе;
- для непрерывного получения обновлений и помощи специалистов продлевается ежегодно.

Дополнительные коммерческие модули Garnet Web Filter, Kaspersky Anti-Virus, Kaspersky Anti-Spam, Kaspersky Suricata Rules Feed могут быть приобретены вместе с основной коммерческой лицензией ИКС или в любой момент использования ИКС.

После окончания срока действия модуля основная лицензия продолжает работать. Однако связанные с модулем функции, обновления или сервисы становятся недоступны.

6.5 Расширение и продление

6.5.1 Расширение лицензии

Если действующего лимита недостаточно, лицензию расширяют до нового общего

количества пользователей.

Например, у заказчика есть лицензия на 100 пользователей, а после увеличения штата их станет 140. Необходимо приобрести расширение лицензии до количества, покрывающего всех 140 пользователей.

Перед расчётом следует проверить:

- текущий лицензионный лимит;
- фактическое количество включённых пользователей;
- планируемый рост;
- производительность оборудования;
- условия лицензирования дополнительных модулей.

После оплаты заказчик получает обновлённую лицензию в интерфейсе ИКС (переустановка программы не требуется).

6.5.2 Продление модулей

Модуль «Техподдержка». В первый год техподдержка предоставляется бесплатно, отдельно оплачивать модуль «Техподдержка» не требуется. Партнеру следует заранее сообщить заказчику о том, что бесплатная подписка заканчивается и предложить платное продление на следующий год.

Если срок действия техподдержки уже закончился, условия возобновления необходимо проверять по актуальному прайс-листу. Для истекшего модуля «Техподдержка» стоимость формируется в зависимости от того, как давно закончилась подписка:

- если продление модуля «Техподдержка» оформляется заранее или в первые 3 месяца после окончания подписки, стоимость составляет 45% от цены коммерческой лицензии по актуальному прайс-листу;
- если модуль «Техподдержка» истек более 3 месяцев назад, стоимость составляет 60% от цены коммерческой лицензии по актуальному прайс-листу;
- если модуль «Техподдержка» истек более 12 месяцев назад, стоимость составляет 80% от цены коммерческой лицензии по актуальному прайс-листу.

Модули Garnet Web Filter, Kaspersky Anti-Virus, Kaspersky Anti-Spam, Kaspersky Suricata Rules Feed. Стоимость новой покупки и продления единая, не зависит от сроков продления. Цена для клиента формируется по актуальному прайс-листу.

Для подготовки предложения на продление следует запросить:

1. Серийный номер ИКС.
2. Текущее количество пользователей.
3. Перечень действующих модулей.
4. Даты окончания их действия.
5. Планируемое расширение лицензии.

Обсуждение продления с клиентом рекомендуется начинать за 3 месяца до окончания текущей подписки, чтобы клиент успел согласовать закупку и не потерял доступ к обновлениям и технической поддержке.

6.6 Перенос лицензии и примеры расчёта

6.6.1 Перенос и восстановление

Лицензия связана с установленной копией ИКС и её серийным номером. После переустановки или переноса системы формируется новый серийный номер, поэтому необходимо получить новый лицензионный ключ.

Порядок действий:

1. Создать резервную копию конфигурации.
2. Сохранить старый и новый серийные номера.
3. Обратиться к менеджеру или в отдел по работе с клиентами.
4. Получить и активировать новую лицензию.
5. Восстановить конфигурацию.

Один лицензионный ключ нельзя одновременно использовать на нескольких установках.

При получении нового лицензионного ключа старый ключ будет удален из системы вендора.

6.6.2 Пример 1. Новая лицензия

Через ИКС доступ в интернет будут получать:

- 80 сотрудников;
- 5 подрядчиков;
- 3 служебные учётные записи.

Расчётное количество — 88 пользователей. Требуется коммерческая лицензия, покрывающая не менее 88 пользователей.

Модуль «Техподдержка» предоставляется бесплатно на первый год. Отдельная плата за него при первоначальной покупке не взимается.

Клиенту можно предложить купить вместе с лицензией ИКС дополнительные модули, это позволит усилить защиту его сети.

6.6.3 Пример 2. Образовательная организация

В ИКС будут включены 60 сотрудников и 400 учащихся. Требуется лицензия не менее чем на 460 пользователей.

Если доступ организован иначе, расчёт необходимо согласовать с техническим специалистом.

Для государственных бюджетных образовательных организаций действуют специальные цены и условия. Возможность их применения следует уточнять у вендора.

6.6.4 Пример 3. Ежегодное продление

Заказчик приобрёл ИКС год назад. Основная лицензия продолжает действовать бессрочно, но бесплатный период техподдержки заканчивается.

Заказчику необходимо предложить платное продление модуля на следующий год, чтобы сохранить доступ к обновлениям, исправлениям и помощи специалистов.

6.6.5 Пример 4. Расширение

У заказчика есть лицензия на 100 пользователей. После расширения штата количество

включённых пользователей увеличится до 135.

Необходимо:

- проверить производительность оборудования – достаточно ли ресурсов для нового количества сотрудников;
- докупить необходимое число пользователей.

Срок действия техподдержки и модулей при расширении лицензии остается неизменным. При продлении необходимо рассчитывать стоимость на новое актуальное число пользователей.

6.6.6 Частые вопросы

Учитываются ли отключённые пользователи?

Нет. Лицензионный лимит занимают только включённые пользователи.

Всегда ли пользователь - это сотрудник?

Нет. Пользователем может быть учётная запись человека, общая учётная запись или отдельный компьютер. Это зависит от организации доступа.

Нужно ли оплачивать техподдержку при покупке ИКС?

Нет. В первый год модуль «Техподдержка» предоставляется бесплатно.

Когда необходимо начинать оплачивать техподдержку?

Со второго года использования ИКС. Для непрерывного доступа к обновлениям и помощи специалистов модуль необходимо продлевать ежегодно.

Прекратит ли ИКС работать после окончания техподдержки?

Нет. Основная бессрочная лицензия продолжит работать. Однако клиент потеряет доступ к новым версиям, обновлениям безопасности и технической помощи.

Почему важно ежегодно продлевать техподдержку?

Регулярное продление позволяет использовать актуальную версию ИКС, получать исправления ошибок и уязвимостей, а также обращаться за помощью к техническим специалистам.

Можно ли увеличить лимит ИКС Lite?

Нет. Для 10 и более пользователей требуется коммерческая лицензия.

Можно ли использовать старый ключ после переустановки?

Серийный номер изменился, необходимо запросить новую лицензию. Количество запросов на новую лицензию не ограничено.

6.7 Физическая и виртуальная установка

6.7.1 Установка на физический сервер

Физическая установка подходит, если заказчику требуется выделенная аппаратная платформа.

Её преимущества:

- ресурсы сервера полностью доступны ИКС;
- сетевые интерфейсы подключаются непосредственно к оборудованию;
- работа не зависит от общей платформы виртуализации;

- проще обеспечить физическое разделение систем.

При подборе сервера необходимо учитывать:

- количество пользователей;
- скорость и количество интернет-каналов;
- объём обрабатываемого трафика;
- количество одновременных соединений;
- использование IDS/IPS и антивирусной проверки;
- объём журналов и отчётов;
- число сетевых сегментов;
- требования к резервированию;
- ожидаемый рост нагрузки.

6.7.2 Установка на виртуальную машину

Виртуальная установка подходит, если у заказчика уже используется поддерживаемая платформа виртуализации и есть достаточные вычислительные ресурсы.

Её преимущества:

- не требуется отдельный физический сервер;
- ресурсы виртуальной машины можно изменять;
- проще выполнять резервное копирование;
- решение можно размещать в существующей виртуальной инфраструктуре.

Необходимо проверить:

- поддержку используемого гипервизора;
- выделенные ресурсы процессора, памяти и диска;
- параметры виртуальных сетевых адаптеров;
- подключение внешних и внутренних сетей;
- отсутствие ограничений со стороны виртуального коммутатора;
- резерв ресурсов на пиковую нагрузку;
- порядок резервного копирования и восстановления.

Ресурсы виртуальной машины не должны выделяться только по формальному минимуму.

Недостаток процессорной мощности, памяти или скорости диска может снизить производительность ИКС.

6.7.3 Требования к серверу

Универсальной конфигурации для всех установок нет. Сервер подбирается с учётом нагрузки и используемых функций.

Основные параметры:

Параметр	Что влияет на подбор
Процессор	Скорость трафика, IDS/IPS, антивирус, число соединений
Оперативная память	Количество пользователей, сервисов и правил
Накопитель	Журналы, отчёты, почта, резервные копии



Параметр	Что влияет на подбор
Сетевые интерфейсы	Количество каналов, сегментов и требуемая скорость
Резерв производительности	Рост пользователей и трафика
Отказоустойчивость	Требования к непрерывности работы

Актуальные минимальные требования следует проверять в технической документации для выбранной версии ИКС. Для каналов высокой скорости, сложной сегментации, кластера или интенсивного анализа трафика конфигурацию должен рассчитать пресейл-инженер.

6.8 Состав поставки и выбор варианта

Точный состав поставки определяется спецификацией и договором.

Элемент поставки	NGWF ИКС	ПАК NGWF ИКС	ИКС ФСТЭК	ПАК ИКС ФСТЭК
Электронные ключи активации для коммерческой лицензии ИКС и дополнительных модулей	+	+	+	+
Электронный файл «Данные личного кабинета»	+	+	+	+
Модуль «Техподдержка» на первый год без дополнительной оплаты	+	+	+	+
Комплект поставки ФСТЭК	-	-	+	+
Аппаратная платформа	-	+	-	+
Гарантийный талон	-	+	-	+

6.8.4 Как выбрать оптимальный вариант

Условия заказчика	Рекомендуемый вариант
Есть подходящий физический сервер	Программная лицензия NGFW ИКС
Есть виртуальная инфраструктура и достаточные ресурсы	Программная лицензия NGFW ИКС
Нет подходящего оборудования	ПАК NGFW ИКС
Нужно программное обеспечение и оборудование одной поставкой	ПАК NGFW ИКС
Требуется ИКС ФСТЭК, но сервер предоставляет заказчик	Программная лицензия ИКС ФСТЭК



Условия заказчика	Рекомендуемый вариант
Техническое задание требует сертифицированный ПАК	Сертифицированный ПАК ИКС ФСТЭК
Требуется высокая доступность	Два узла и отказоустойчивая конфигурация

6.8.5 Порядок выбора

1. Определить, требуется ли сертифицированное решение.
2. Проверить наличие подходящего сервера или виртуальной инфраструктуры.
3. Рассчитать необходимую производительность.
4. Определить количество сетевых интерфейсов.
5. Уточнить требования к отказоустойчивости.
6. Проверить условия технического задания.
7. Выбрать программную поставку, ПАК или сертифицированный ПАК.
8. Согласовать состав оборудования и документов.
9. Проверить итоговую спецификацию с техническим специалистом.

Оптимальный вариант — не обязательно самый дорогой или самый производительный. Он должен соответствовать задачам заказчика, требованиям проекта и предполагаемой нагрузке без необоснованных затрат.

Если характеристики инфраструктуры или требования к сертификации неясны, спецификацию нельзя формировать на основании предположений. Необходимо запросить дополнительные сведения и привлечь пресейл-инженера вендора.

7. Процесс продажи ИКС

Продажа ИКС строится вокруг задачи заказчика: сначала партнёр выясняет потребность и параметры проекта, затем подтверждает соответствие решения, организует проверку продукта и готовит предложение. После поставки работа продолжается через продление модулей и развитие заказчика.

7.1 Основные этапы продажи

7.1.1 Найти потенциального заказчика

ИКС следует предлагать организациям, которым требуется:

- защита сетевого периметра;
- контроль доступа пользователей и трафика;
- замена зарубежного межсетевого экрана;
- сертифицированное ФСТЭК решение;
- программная поставка или готовый ПАК;
- объединение нескольких сетевых функций в одном продукте.

Подробнее целевые заказчики и признаки потребности описаны в разделе 4.

7.1.2 Установить контакт и выявить потребность

Во время первого разговора необходимо кратко представить ИКС и перейти к вопросам о задачах заказчика.

Минимально следует уточнить:

- какую задачу необходимо решить;
- что используется сейчас;
- почему рассматривается замена или новая закупка;
- сколько пользователей и какая скорость каналов;
- какие функции обязательны;
- требуется ли сертификат ФСТЭК;
- когда планируется закупка;
- кто участвует в выборе решения.

На этом этапе важно не перечислять все возможности ИКС, а определить, соответствует ли продукт проекту.

7.1.3 Зарегистрировать проект

Если партнёр ведёт конкурсную закупку или прямую поставку лицензии от 100 пользователей, проект необходимо зарегистрировать у вендора.

В заявке указываются заказчик, задача, предполагаемый состав решения, сроки и подтверждение работы над проектом. Регистрация действует до трёх месяцев и при необходимости может быть продлена.

Регистрация помогает закрепить проект за партнёром и получить поддержку вендора при подготовке сделки.

7.1.4 Подтвердить соответствие решения

После квалификации необходимо подобрать редакцию, количество пользователей, вариант поставки, производительность и дополнительные модули.

Если требования сложные или исходных данных недостаточно, следует привлечь пресейл-инженера. Порядок подбора решения описан в разделе 7.

7.1.5 Провести демонстрацию или тестирование

Демонстрация используется, чтобы показать возможности ИКС на примере задач заказчика. Если требуется проверить производительность, совместимость, сетевую схему или отдельные функции, организуется тестирование. До его начала необходимо согласовать:

- задачи и критерии успешного результата;
- тестовую схему;
- проверяемые функции;
- сроки;
- ответственных со стороны партнёра и заказчика.

По завершении результаты следует зафиксировать. Тестирование без заранее определённых критериев может затянуть сделку и не дать заказчику основания для выбора.

Для проектов от 100 пользователей можно запросить демонстрацию или тестирование ИКС с участием пресейл-инженеров вендора.

7.1.6 Подготовить предложение

Коммерческое предложение должно соответствовать подтверждённым требованиям заказчика и содержать:

- состав решения;
- количество пользователей;
- редакцию и вариант поставки;
- дополнительные модули;
- стоимость;
- сроки и условия поставки;
- условия технической поддержки.

Перед отправкой необходимо проверить спецификацию, актуальность цен и соответствие условиям партнёрской программы.

7.1.7 Закрывать сделку

На завершающем этапе необходимо согласовать итоговую спецификацию, условия закупки и сроки поставки.

Перед оформлением заказа следует убедиться, что:

- требования заказчика не изменились;
- спецификация проверена;
- возражения проработаны;
- порядок оплаты и поставки согласован;
- определены дальнейшие действия после получения продукта.

Продажа считается завершённой не после отправки предложения, а после оформления заказа и выполнения согласованных обязательств.

7.2 Краткая схема продажи

Этап	Результат
Поиск и первый контакт	Найден потенциальный заказчик и установлен контакт
Квалификация	Понятны задача, параметры проекта, сроки и участники выбора
Регистрация проекта	Проект зарегистрирован, если соответствует условиям программы
Подбор решения	Определены редакция, лицензия, поставка и модули
Демонстрация или тестирование	Заказчик убедился, что решение соответствует его задачам
Коммерческое предложение	Передана проверенная спецификация с ценой и условиями
Заккрытие сделки	Заказ оформлен, условия поставки согласованы

На каждом этапе должен быть определён следующий шаг: встреча, получение исходных данных, демонстрация, тестирование, отправка предложения или оформление заказа. Если следующего шага нет, сделка фактически не продвигается.

7.3 Продление и развитие заказчика

После первой поставки партнёру необходимо поддерживать связь с заказчиком и отслеживать:

- ввод ИКС в эксплуатацию;
- окончание срока действия дополнительных модулей и техподдержки;
- увеличение количества пользователей;
- появление новых филиалов и сетевых сегментов;
- потребность в дополнительных модулях;
- необходимость обновления оборудования или организации отказоустойчивости.

При появлении соответствующей задачи партнер получает возможность развить клиента и увеличить чек ежегодных сделок. Это может быть расширение лицензии, продление модулей, подключение Garnet Web Filter, антивируса, антиспама или правил Suricata, поставка ПАК, внедрение кластера.

При продлении и развитии заказчика приоритет поставки сохраняется за партнёром, выполнившим предыдущую поставку, при соблюдении условий партнёрской программы.

Главная задача после продажи — не просто напомнить о продлении, а своевременно выявить изменения в инфраструктуре заказчика и предложить решение, соответствующее новым требованиям.

8. Скрипты и инструменты продаж

Скрипт помогает вести разговор, но не заменяет диалог. Менеджер сначала выясняет ситуацию заказчика, затем связывает ИКС с его задачей и договаривается о следующем шаге. Нельзя обещать функцию, производительность, скидку или соответствие требованиям без проверки.

8.1 Краткий рассказ об ИКС

ИКС — российский NGFW для защиты сети и управления интернет-трафиком. Он контролирует соединения, доступ к сайтам и приложениям, помогает обнаруживать сетевые атаки и ведёт журналы событий. Решение поставляется как программа или ПАК; для регулируемых систем предусмотрена редакция ИКС ФСТЭК. Конфигурация подбирается по задачам, количеству пользователей, скорости каналов и необходимым функциям.

8.2 Схема первого звонка

Этап	Задача менеджера	Пример формулировки
Контакт	Представиться и получить согласие на разговор	«Добрый день, [имя]. Меня зовут [имя], компания [партнёр].»
Роль	Убедиться, что выбран нужный специалист	«Правильно понимаю, что с вами можно обсудить защиту сети и межсетевые экраны?»
Ситуация	Понять, что используется сейчас	«Какое решение защищает сеть сейчас? Оно российское или зарубежное?»
Проблема	Найти неудовлетворённую задачу	«Что в текущем решении хотелось бы улучшить: функции, производительность, поддержку или стоимость?»
Последствия	Понять важность проблемы	«К чему приводят сбои или ограничения: простоям, дополнительной работе, рискам или затратам?»
Ценность	Проверить интерес к изменению	«Насколько полезно было бы проверить российское решение с поддержкой специалистов?»
Квалификация	Собрать ключевые параметры	Пользователи, каналы, функции, сертификация, сроки, инфраструктура
Следующий шаг	Зафиксировать действие и срок	«Предлагаю [опросный лист / ВКС / тестирование / расчёт]. Когда удобно продолжить?»

8.2.1 Разговор через секретаря

«Добрый день! Подскажите, кто отвечает за корпоративную сеть и её защиту?»

Если просят прислать материалы, уточните имя и контакты ответственного специалиста и договоритесь, когда можно вернуться к обсуждению. Не нужно подробно презентовать продукт секретарю.

8.3 Вопросы по модели СПИН

Блок	Что выяснить	Примеры вопросов
Ситуация	Текущая защита и критерии выбора	Что используется? Как давно? Какие задачи закрывает? Требуется ли сертификат ФСТЭК?
Проблема	Ограничения текущего подхода	Какие задачи закрыты не полностью? Бывают ли сбои? Доступна ли поддержка, когда она нужна?
Последствия	Влияние проблемы	Сколько времени занимает устранение? Чем опасен простой или инцидент для работы и репутации?
Ценность решения	Желаемый результат	Насколько важны понятное управление, российская поддержка, снижение простоев и возможность проверить продукт?

Не задавайте все вопросы подряд. Выбирайте только те, которые логично продолжают ответ собеседника.

8.4 Ветвление разговора

Ситуация заказчика	Уточнение	Следующий шаг
Использует конкурента	Что устраивает и что хотелось бы улучшить? Когда пересматривают решение?	Сравнение по задаче, ВКС или контакт к сроку пересмотра
Решения нет	Как сейчас организован доступ? Какие риски или ограничения нужно снять?	Опросный лист и предварительный подбор
Уже знает ИКС	Было ли тестирование или ВКС? Почему проект не состоялся?	Вернуться к изменившейся задаче и срокам
Просит письмо	Что актуальнее: обзор, замена решения или ИКС ФСТЭК?	Отправить подходящий материал и назначить повторный контакт
Потребности нет	Когда обычно пересматривают защиту сети?	Получить согласие на контакт в подходящий срок

8.5 Квалификация проекта

Зафиксируйте задачу, текущее решение, обязательные функции, количество пользователей, скорость каналов, тип системы, необходимость сертификата ФСТЭК, вариант размещения, отказоустойчивость, сроки, бюджет, участников выбора и конкурентов.

Завершите проверкой понимания:

«Правильно ли я понял, что вам нужно [задача], важно [требования], а решение планируется принять до [срок]?»

8.6 ВКС и тестирование

В проектах от 100 пользователей можно подключить пресейл-инженера вендора, провести ВКС и организовать тестирование.

Формат	Когда использовать	Что подготовить
ВКС / демонстрация	Заказчик хочет увидеть интерфейс и обсудить функции	Задачи, участники, список вопросов, желаемые сценарии
Техническая консультация	Нужен расчёт, проверка схемы или интеграции	Опросный лист, схема сети, требования и предварительная спецификация
Тестирование	Нужно подтвердить совместимость, функции или работу в инфраструктуре	Цель, стенд, сценарии, ответственные, сроки и критерии успеха

В конце встречи обязательно согласуйте следующее действие: заполнение опросного листа, запуск пилота, расчёт или подготовку предложения.

8.7 Чек-лист менеджера

До звонка	изучить организацию и историю контактов
	определить цель звонка и пять основных вопросов
	подготовить полезный следующий шаг
Во время звонка	сначала спрашивать, затем презентовать
	записывать цифры и требования дословно
	не придумывать технические ответы
	кратко повторить задачу и согласовать действие со сроком
После звонка	зафиксировать сведения в CRM
	отправить обещанные материалы
	назначить следующий контакт
	при необходимости зарегистрировать проект и привлечь пресейл-инженера

9. Работа с возражениями

Возражение не всегда означает отказ. Часто заказчику не хватает информации, он не видит оснований для изменений или пока не готов перейти к следующему этапу.

Менеджеру следует:

1. Выслушать заказчика.
2. Уточнить причину возражения.
3. Связать ответ с его задачей.
4. Предложить конкретное следующее действие.

Не нужно спорить, критиковать конкурентов или сразу предлагать скидку.

9.1 «У нас уже есть межсетевой экран»

Наличие межсетевого экрана не исключает потребности в новом решении. Важно понять, устраивает ли заказчика используемый продукт и планируется ли его замена.

«Понимаю. Подскажите, вы планируете продолжать использовать текущее решение или рассматриваете замену, обновление либо резервный вариант?»

Если замена не планируется:

«Когда обычно пересматривается решение или заканчивается срок его поддержки? Мы можем вернуться к обсуждению ближе к этой дате.»

Если есть сложности:

«Какие задачи текущее решение закрывает недостаточно хорошо?»

После ответа можно предложить демонстрацию, сравнение по требованиям или тестирование ИКС.

9.2 «Нас устраивает текущее решение»

Не следует убеждать заказчика, что его продукт плохой. Необходимо выяснить, какие качества он особенно ценит и есть ли основания для будущего пересмотра.

«Это хорошо. Подскажите, что для вас особенно важно в текущем решении: функциональность, производительность, удобство управления, поддержка или стоимость?»

Затем:

«Планируются ли изменения в инфраструктуре, новые требования или пересмотр решения в ближайшее время?»

Если потребности нет, следует согласовать срок следующего контакта и не настаивать на немедленной замене.

9.3 «Слишком дорого»

Сначала необходимо понять, с чем заказчик сравнивает стоимость и соответствует ли предложение его задаче.

«Подскажите, пожалуйста, стоимость выше запланированного бюджета или вы сравниваете

её с другим предложением?»

Дополнительно следует уточнить:

- одинаковы ли составы решений;
- включено ли оборудование;
- совпадают ли количество пользователей и сроки;
- нужны ли все предложенные модули;
- учтены ли внедрение, сопровождение и дальнейшая эксплуатация.

После проверки:

«Давайте ещё раз сверим состав. Возможно, в предложение включены функции или вариант поставки, которые вам не требуются. Если состав подобран верно, я поясню, из чего складывается стоимость.»

Нельзя обещать скидку до согласования.

9.4 «У конкурента дешевле»

Сравнивать нужно не только итоговую сумму, но и одинаковые условия поставки.

«Подскажите, пожалуйста, какое решение вы сравниваете с ИКС и что входит в предложение конкурента?»

Необходимо проверить:

- количество пользователей;
- программную или аппаратную поставку;
- необходимые функции и модули;
- наличие требуемой сертификации;
- сроки лицензий и поддержки;
- стоимость расширения и дальнейшего сопровождения.

После уточнения:

«Если составы сопоставимы, мы сможем предметно обсудить разницу. Если они отличаются, сначала приведём предложения к одинаковым требованиям.»

Не следует утверждать, что ИКС всегда выгоднее.

9.5 «Мы рассматриваем другое российское решение»

Это означает, что задача существует и заказчик находится на этапе выбора.

«Хорошо. Подскажите, пожалуйста, какие решения вы рассматриваете и по каким критериям будете выбирать?»

Далее необходимо выяснить:

- какие функции обязательны;
- требуется ли сертификат ФСТЭК;
- какие показатели производительности важны;
- нужен ли ПАК;
- планируется ли тестирование;
- кто принимает итоговое решение.

После ответа:

«Предлагаю проверить ИКС по тем же критериям. Мы можем провести демонстрацию или организовать тестирование по заранее согласованным сценариям.»

Не нужно строить разговор на критике другого российского продукта.

9.6 «Нам достаточно бесплатного решения»

Бесплатное решение может подходить для отдельных задач. Важно понять, насколько критична защищаемая инфраструктура и какие требования предъявляются к продукту.

«Подскажите, пожалуйста, какие задачи закрывает бесплатное решение и чего вы ожидаете от него в дальнейшем?»

Следует уточнить:

- кто отвечает за настройку и обновление;
- требуется ли техническая поддержка;
- нужны ли отчёты, интеграции и централизованное управление;
- допустимы ли простои;
- установлены ли требования к сертификации;
- планируется ли рост инфраструктуры.

После ответа:

«Если текущее решение закрывает все задачи и риски для вас приемлемы, замена может быть не нужна. Если важны сопровождение, предсказуемые обновления или дополнительные функции, стоит сравнить полную стоимость и возможности вариантов.»

9.7 «Не хотим менять привычный продукт»

Основная причина такого возражения — риски перехода, необходимость переноса настроек и обучения сотрудников.

«Понимаю. Что вызывает наибольшие опасения: перенос правил, время внедрения, обучение администратора или возможный простой?»

После уточнения:

«Предлагаю не принимать решение о переходе сразу. Сначала можно провести демонстрацию и проверить основные сценарии на тестовом стенде. Так вы оцените интерфейс и объём необходимых работ.»

Не следует обещать, что переход будет быстрым и полностью автоматическим, пока не изучена текущая конфигурация.

9.8 «У нас нет специалиста для администрирования»

Необходимо понять, кто сейчас отвечает за сеть и какой объём работ заказчик может выполнять самостоятельно.

«Подскажите, кто сейчас обслуживает сеть и используемое средство защиты: штатный сотрудник, подрядчик или внешняя ИТ-компания?»

Затем:

«Какие операции потребуется выполнять регулярно: создавать правила, просматривать события, добавлять пользователей или обновлять систему?»

После ответа можно предложить:

- демонстрацию интерфейса;
- консультацию технического специалиста;
- обучение ответственного сотрудника;
- внедрение с участием партнёра;
- дальнейшее сопровождение.

Нельзя обещать, что техническая поддержка возьмёт на себя полное администрирование без согласования условий.

9.9 «Слишком сложно внедрять»

Сложность зависит от инфраструктуры, требований и объёма переносимых настроек.

«Подскажите, пожалуйста, что именно кажется сложным: установка, перенос правил, интеграция с каталогом пользователей, переключение трафика или обучение сотрудников?»

После ответа:

«Предлагаю сначала оценить объём работ. Для этого потребуется схема сети, сведения о текущем решении и основные требования. Затем технический специалист сможет предложить порядок внедрения.»

Для сложных проектов целесообразно предусмотреть тестовый стенд, поэтапный переход и план возврата к прежней схеме.

9.10 «Нет бюджета»

Отсутствие бюджета отличается от возражения по цене. Заказчик может считать решение подходящим, но не иметь возможности приобрести его сейчас.

«Понимаю. Бюджет на эту задачу не предусмотрен совсем или его планируют сформировать позднее?»

Далее следует уточнить:

- когда начинается бюджетное планирование;
- на какой период возможна закупка;
- требуется ли предварительный расчёт;
- кто согласовывает бюджет;
- сохраняется ли актуальность задачи.

После ответа:

«Тогда подготовим ориентировочный состав решения, чтобы вы могли учесть его при планировании, и вернёмся к обсуждению [дата].»

Не следует снижать цену, если причина заключается не в стоимости, а в отсутствии финансирования.

9.11 «Не готовы тестировать»

Необходимо понять, почему заказчик отказывается: нет времени, специалиста, инфраструктуры или критериев проверки.

«Подскажите, пожалуйста, что мешает тестированию сейчас: нехватка времени, отсутствие ответственного специалиста или пока нет необходимости проверять продукт?»

Если достаточно демонстрации:

«Тогда предлагаю начать с короткой демонстрации нужных функций. После неё вы сможете решить, требуется ли полноценное тестирование.»

Если нет ресурсов:

«Можно ограничить проверку двумя-тремя наиболее важными сценариями и заранее согласовать необходимое участие с вашей стороны.»

Если задача пока не сформирована, тестирование лучше перенести и согласовать дату следующего контакта.

9.12 «Нам не нужна сертифицированная версия»

Сертифицированную редакцию не следует предлагать без подтверждённой необходимости.

«Понимаю. Для какой сети или информационной системы приобретается решение? Есть ли требование о применении сертифицированного межсетевого экрана в техническом задании или проекте защиты?»

Если сертификат не требуется:

«В таком случае можно рассматривать обычную редакцию NGFW ИКС. Она подходит для корпоративных сетей, где применение сертифицированного ФСТЭК средства не установлено требованиями проекта.»

Наличие персональных данных само по себе не означает обязательного применения ИКС ФСТЭК.

9.13 «Нужен продукт более высокого класса»

Сначала необходимо выяснить, что заказчик понимает под более высоким классом.

«Подскажите, пожалуйста, что именно вы имеете в виду: требуемый класс или профиль защиты, производительность, масштаб инфраструктуры либо набор функций?»

Если речь идёт о сертификации, необходимо проверить требования технического задания и проекта защиты.

Если речь идёт о производительности или масштабе:

«Давайте зафиксируем требуемые параметры и передадим их техническому специалисту. После проверки мы честно сообщим, соответствует ли ИКС проекту.»

Если ИКС не подходит по обязательным требованиям, не следует пытаться продолжать продажу любой ценой.

9.14 «Вернёмся к вопросу позже»

Фраза «позже» должна быть переведена в понятную причину и конкретный срок.

«Конечно. Подскажите, пожалуйста, с чем связана пауза: бюджетом, сроками проекта, внутренним согласованием или другими приоритетами?»

Затем:

«Когда лучше вернуться к обсуждению: в [месяц] или после [событие]?»

Перед завершением разговора необходимо уточнить:

- сохраняется ли задача;
- что должно произойти до следующего контакта;
- какие материалы нужны заказчику;
- кто будет участвовать в дальнейшем обсуждении.

В CRM следует поставить задачу на согласованную дату и зафиксировать причину переноса.

9.15 Ошибки при отработке возражений

9.15.1 Спорить с заказчиком

Фразы «вы ошибаетесь» или «это не так» вызывают сопротивление. Сначала необходимо понять основания его позиции.

9.15.2 Отвечать до уточнения причины

Одинаковое возражение может иметь разные причины. «Дорого» может означать отсутствие бюджета, более дешёвое предложение конкурента или избыточный состав спецификации.

9.15.3 Перегружать ответ функциями

Длинный список возможностей не устраняет сомнение. Следует говорить только о том, что связано с задачей заказчика.

9.15.4 Сразу предлагать скидку

Скидка не поможет, если заказчику не нужен продукт, не подходит конфигурация или отсутствует бюджет.

9.15.5 Критиковать конкурентов

Нельзя распространять неподтверждённые сведения или обесценивать выбор заказчика. Сравнение должно строиться по требованиям, составу поставки и результатам тестирования.

9.15.6 Давать неподтверждённые обещания

Нельзя обещать производительность, совместимость, сроки внедрения, функции или скидки без проверки.

9.15.7 Давить на заказчика

Возражение не нужно «побеждать». Цель менеджера — понять ситуацию и определить разумный следующий шаг.

9.15.8 Игнорировать неподходящие требования

Если ИКС не соответствует обязательному требованию, это необходимо честно сообщить после технической проверки.

9.15.9 Не договариваться о следующем действии

Разговор должен завершаться конкретным шагом:

- отправкой материалов;
- демонстрацией;
- технической консультацией;
- заполнением опросного листа;
- тестированием;
- подготовкой предложения;
- повторным контактом в согласованную дату.

9.15.10 Не фиксировать причину в CRM

Необходимо записывать фактическую причину возражения, ответ заказчика, договорённость и дату следующего контакта. Формулировка «клиент думает» не позволяет продолжить работу качественно.

Главное правило: сначала понять причину возражения, затем дать связанный с ней ответ и предложить следующий шаг.

10. Техническая поддержка

Техническая поддержка помогает пользователям устанавливать, настраивать и устранять проблемы в работе ИКС. Она не заменяет системного администратора и не распространяется на обслуживание сети, оборудования и программ сторонних производителей.

10.1 Виды технической поддержки

10.1.1 Поддержка в течение первого года

После первой покупки ИКС заказчик получает персональную техническую поддержку на один год.

10.1.2 Модуль «Техподдержка»

После окончания первого года для продолжения персональной помощи необходимо приобрести модуль «Техподдержка».

В рамках модуля специалисты:

- консультируют по установке и настройке ИКС;
- помогают определить причины проблем в работе продукта;
- анализируют сообщения об ошибках, скриншоты и журналы событий;
- при необходимости подключаются к ИКС удалённо по SSH;
- передают сложные вопросы специалистам разработки.

Техническая поддержка не выполняет постоянное администрирование ИКС, сети заказчика или сторонних решений.

10.1.3 Поддержка тестирования и партнёров

Пользователи тестовых лицензий, партнёры и дистрибьюторы также могут обращаться за консультациями.

10.1.4 Когда в поддержке могут отказать

Помощь может не предоставляться, если:

- отсутствует коммерческая или тестовая лицензия;
- лицензия рассчитана менее чем на 30 пользователей;
- используется неподдерживаемая версия ИКС;
- заявитель не предоставил сведения, необходимые для диагностики;
- проблема относится к стороннему оборудованию или программному обеспечению.

10.2 Как создать обращение

Обращаться в техническую поддержку следует по вопросам регистрации, установки, настройки и устранения проблем в работе ИКС.

В обращении необходимо указать:

- название организации и ИНН;
- имя и контакты заявителя;
- полную версию ИКС;
- краткое описание проблемы;

- когда и после каких действий она появилась;
- какой результат ожидался и какой результат получен;
- повторяется ли проблема;
- какие действия уже предпринимались.

К обращению желательно приложить:

- скриншоты ошибки;
- точный текст сообщения;
- журналы событий;
- время возникновения проблемы;
- схему подключения, если она имеет значение;
- последовательность действий для воспроизведения.

Не следует отправлять пароли и другие секретные данные в открытом виде.

После регистрации обращению присваивается номер. Его необходимо сохранять и указывать при последующем общении.

10.2.1 Пример описания

Перестал работать доступ пользователей в интернет. Проблема появилась [дата и время], воспроизводится постоянно. Перезапуск службы результата не дал. Прилагаем скриншот, журналы событий и описание сетевой схемы.

Чем точнее описана ситуация, тем быстрее специалист сможет приступить к диагностике.

10.3 Приоритеты и обработка обращений

Обращения обрабатываются с учётом приоритета клиента и характера проблемы.

Приоритетную персональную поддержку получают:

- заказчики в течение первого года после первой покупки;
- заказчики с действующим модулем «Техподдержка».

Отдельно обрабатываются обращения пользователей тестовых лицензий, партнёров и дистрибьюторов.

Максимальное время первоначального ответа по регламенту — 10 рабочих часов. Это срок реакции специалиста, а не гарантированный срок полного решения проблемы.

10.3.1 Как проходит работа

1. Обращение регистрируется и получает номер.
2. Специалист проверяет описание и исходные данные.
3. При необходимости запрашиваются дополнительные сведения, журналы или удалённый доступ.
4. Специалист проводит диагностику и предлагает решение.
5. Если вопрос невозможно решить на текущем уровне, он передаётся более квалифицированному специалисту или в отдел разработки.
6. Пользователю сообщают результат либо дальнейший порядок действий.

Передача вопроса в разработку не означает, что исправление обязательно войдёт в ближайшее обновление. Возможность и сроки изменений определяются после анализа.



10.4 Обновления и работа с уязвимостями

Обновления ИКС могут содержать:

- исправления ошибок;
- устранение выявленных уязвимостей;
- улучшения стабильности;
- изменения функций;
- обновление отдельных компонентов.

Перед обновлением необходимо:

1. Проверить, поддерживается ли переход с установленной версии.
2. Изучить описание изменений.
3. Создать резервную копию конфигурации.
4. Проверить наличие свободных ресурсов.
5. Выбрать время с минимальным влиянием на работу организации.
6. Для критичной инфраструктуры предусмотреть план возврата.

Нельзя начинать обновление без резервной копии и оценки возможного простоя.

10.4.1 Работа с уязвимостями

Разработчик анализирует сведения об уязвимостях, определяет затронутые версии и при необходимости выпускает исправления или рекомендации.

Если заказчик обнаружил возможную уязвимость, в обращении следует указать:

- версию ИКС;
- затронутый компонент;
- условия воспроизведения;
- возможные последствия;
- журналы, скриншоты или иные подтверждения;
- контакт технического специалиста.

Сведения о возможной уязвимости не следует публиковать до получения ответа разработчика. Это необходимо, чтобы проверить информацию и подготовить меры защиты.

10.5 Частые технические вопросы

10.5.1 Техническая поддержка настроит ИКС вместо заказчика?

Нет. Специалисты консультируют и помогают устранить проблемы, но не выполняют постоянное администрирование системы.

10.5.2 Поддержка помогает со сторонним оборудованием?

Только в части, необходимой для диагностики работы ИКС. Настройка коммутаторов, маршрутизаторов, операционных систем и других продуктов не входит в поддержку.

10.5.3 Можно ли обратиться без модуля «Техподдержка»?

Персональная помощь предоставляется в течение первого года после покупки или при наличии действующего модуля. Другие случаи рассматриваются по условиям регламента.

10.5.4 Поддерживается ли старая версия ИКС?

Поддержка предоставляется только для версий, указанных в действующем регламенте. Перед обращением необходимо проверить актуальность используемой версии.

10.5.5 Зачем предоставлять журналы событий?

Они помогают определить время, причину и последовательность возникновения проблемы. Без журналов диагностика может быть невозможна.

10.5.6 Обязательно ли предоставлять удалённый доступ?

Не всегда. Он запрашивается, если предоставленных материалов недостаточно. Если доступ предоставить невозможно, следует согласовать другой способ диагностики.

10.5.7 Что означает срок ответа 10 рабочих часов?

Это максимальное время первоначальной реакции на обращение. Специалисты отвечают на заявки значительно быстрее. Например, среднее время ответа в онлайн-чате составляет 30 секунд. Срок полного решения зависит от сложности проблемы, полноты сведений и необходимости участия разработчиков.

10.5.8 Что делать перед обновлением?

Изучить описание версии, создать резервную копию, проверить порядок перехода и запланировать возможный перерыв в работе.

10.5.9 Что делать, если вопрос долго не решается?

Указать номер обращения и запросить его текущий статус. Если требуется дополнительная эскалация, она выполняется внутри технической поддержки.

Главное правило: обращение должно содержать достаточно сведений для воспроизведения и диагностики проблемы.



11. Коммерческие и маркетинговые материалы

Название файла	Содержание
1. Буклеты ФСТЭК	
Буклет ИКС RF50_ФСТЭК	Описание сертифицированного ФСТЭК программно-аппаратного комплекса ИКС, подходящего для организаций до 50 пользователей. В буклете указаны требования Приказа ФСТЭК №117, выполнение которых обеспечивает ИКС.
Буклет ИКС RF700_ФСТЭК	Описание сертифицированного ФСТЭК программно-аппаратного комплекса ИКС, подходящего для организаций до 500 пользователей. В буклете указаны требования Приказа ФСТЭК №117, выполнение которых обеспечивает ИКС.
Буклет ИКС RF1000_ФСТЭК	Описание сертифицированного ФСТЭК программно-аппаратного комплекса ИКС, подходящего для организаций до 1000 пользователей. В буклете указаны требования Приказа ФСТЭК №117, выполнение которых обеспечивает ИКС.
Буклет Межсетевой экран ИКС ФСТЭК	Описание сертифицированного межсетевого экрана ИКС ФСТЭК. В буклете описаны функции продукта, модули, но не указаны требования Приказа №117, выполнение которых обеспечивает ИКС. В буклет включены все доступные для ИКС ФСТЭК аппаратные платформы.
2. Буклеты и листовка NGFW ИКС	
Буклет NGFW ИКС	Описание функционала NGFW ИКС, специальных служб, дополнительных модулей и всех аппаратных платформ, с которыми может быть поставлено данное решение в случае, если клиент хочет приобрести ПАК, а не только ПО.
Буклет ПАК NGFW ИКС RF50	Описание функционала NGFW ИКС, специальных служб и дополнительных модулей. В буклете представлена аппаратная



Название файла	Содержание
	платформа до 50 пользователей. Буклет можно предоставлять клиентам с аналогичным числом юзеров, кому не нужно соблюдать требования ФСТЭК.
Буклет ПАК NGFW ИКС R150	Описание функционала NGFW ИКС, специальных служб и дополнительных модулей. В буклете представлена аппаратная платформа до 150 пользователей. Буклет можно предоставлять клиентам с аналогичным числом юзеров, кому не нужно соблюдать требования ФСТЭК.
Буклет ПАК NGFW ИКС R300	Описание функционала NGFW ИКС, специальных служб и дополнительных модулей. В буклете представлена аппаратная платформа до 300 пользователей. Буклет можно предоставлять клиентам с аналогичным числом юзеров, кому не нужно соблюдать требования ФСТЭК.
Буклет ПАК NGFW ИКС RF700	Описание функционала NGFW ИКС, специальных служб и дополнительных модулей. В буклете представлена аппаратная платформа до 500 пользователей. Буклет можно предоставлять клиентам с аналогичным числом юзеров, кому не нужно соблюдать требования ФСТЭК.
Буклет ПАК NGFW ИКС RF1000	Описание функционала NGFW ИКС, специальных служб и дополнительных модулей. В буклете представлена аппаратная платформа до 1000 пользователей. Буклет можно предоставлять клиентам с аналогичным числом юзеров, кому не нужно соблюдать требования ФСТЭК.
Листовка NGFW ИКС	Краткое описание функционала NGFW ИКС, дополнительных модулей к нему и ключевых преимуществ использования для быстрого ознакомления с продуктом.
3. Встроенные модули	
Листовка Контент-фильтр ИКС	Предоставляется клиентам, которых



Название файла	Содержание
	интересует контентная фильтрация для ознакомления с возможностями модуля. В листовке также указаны все функции ИКС. Данная листовка чаще всего предоставляется образовательным организациям, так как им необходимо защищать учеников от вредоносного контента.
Листовка Модуль IP-телефонии в ИКС	Описание модуля IP-телефонии, доступного для NGFW ИКС. Используется для аргументации перехода на использование данного модуля со стороннего сервиса IP-телефонии с целью сокращения расходов клиента.
Листовка Почтовый сервер ИКС	Описание почтового сервера, доступного для NGFW ИКС. Используется для аргументации перехода на использование данного модуля со стороннего сервиса с целью сокращения расходов клиента.
4. Дополнительные модули	
Листовка Антивирус	Описание дополнительного модуля – Антивируса Касперского, разработанного специально для NGFW ИКС. Предоставляется клиентам с целью предложения антивирусной защиты на шлюзе.
Листовка Антиспам	Описание дополнительного модуля – Антиспама Касперского, разработанного специально для NGFW ИКС. Предоставляется клиентам, использующим почтовый сервер ИКС, либо SMTP-релей на ИКС, с целью предложения защиты от спама.
Листовка Правила Касперского для Suricata	Описание дополнительного модуля – Правила Касперского для IDS/IPS. Предоставляется клиентам, использующим NGFW ИКС и ИКС ФСТЭК. Обеспечивает защиту от новейших угроз.
Листовка Модули Касперского (общая)	Описание всех трех модулей от Лаборатории Касперского для ИКС. Предоставляется преимущественно для клиентов, покупающих



Название файла	Содержание
	несертифицированный NGFW ИКС, так как все эти модули подходят именно для этого решения.
Листовка Модуль категоризации трафика Garnet	Описание веб-фильтра Garnet, разработанного вендором ИКС совместно с «Лабораторией Касперского» специально для несертифицированного NGFW ИКС. Решение позволяет гибче категоризировать трафик, в файле перечислены доступные категории.
5. Модуль Техподдержка (МТП)	
Листовка Модуль Техподдержка	Содержит аргументацию для ежегодного приобретения модуля «Техподдержка» - продления доступа к техподдержке и получения обновлений продукта.
6. Описание функционала ИКС	
Возможности NGFW ИКС	Подробное описание функций NGFW ИКС, подходящих аппаратных платформ, условий приобретения и продления продукта, а также получения технической поддержки.
Возможности NGFW ИКС ФСТЭК (межсетевого экрана ИКС ФСТЭК)	Подробное описание функций сертифицированного NGFW ИКС ФСТЭК, подходящих аппаратных платформ, условий приобретения и продления продукта, а также получения технической поддержки.
Возможности межсетевого экрана ИКС ФСТЭК и NGFW ИКС	Подробное описание функций двух продуктов в виде сравнительной таблицы, которая позволяет клиентам понять различие между решениями. Файл содержит перечень аппаратных платформ, подходящих для обоих продуктов, условий приобретения и продления продукта, а также получения технической поддержки.
Какие требования Приказа 117 обеспечивает ИКС ФСТЭК	Файл предназначен для клиентов, которым необходимо выполнить требования Приказа ФСТЭК №117. Документ содержит полный перечень мер, установленных п. 63 Приказа №117 с описанием механизма реализации этих мер в

Название файла	Содержание
	NGFW ИКС ФСТЭК.
7. Презентации	
Презентация ИКС для клиентов - 2026	Содержит описание двух продуктов, позволяющее клиенту понять, какое именно решение ИКС ему подходит: назначение, соответствие требованиям регуляторов, совместимость, сценарии использования, дополнительные модули, аппаратные платформы, преимущества ИКС, отзывы клиентов и этапы приобретения NGFW от отправления запроса до активации коммерческой лицензии.
Презентация Почтовый сервер ИКС_2026	Описание почтового сервера, модуля доступного для NGFW ИКС. Данная презентация используется как альтернатива аналогичной листовки для клиентов, которым нужна более подробная информация.
8. Чек-листы	
Чек-лист для тестирования ИКС	Чек-лист поможет последовательно проверить основные возможности ИКС во время тестирования: от базовой настройки и сетевых функций до фильтрации трафика, VPN, контроля пользователей и др. Используйте его, чтобы ничего не упустить и оценить, насколько ИКС подходит для вашей инфраструктуры и задач.
9. Опросный лист ИКС	
Опросный лист ИКС	Документ, который необходимо отправить для заполнения клиентам. чтобы подготовить индивидуальную презентацию и коммерческое предложение.

12. Словарь терминов

Термин	Простое объяснение
AD	Microsoft Active Directory — каталог пользователей, компьютеров и групп организации
Антиспам	Средство выявления нежелательных почтовых сообщений
АСУ ТП	Автоматизированная система управления технологическим процессом
ГИС	Государственная информационная система
Двухфакторная аутентификация (2FA)	Вход по паролю и дополнительному подтверждению
ИКС	«Интернет Контроль Сервер» — продукт для защиты сети и управления трафиком
ИКС ФСТЭК	Сертифицированная редакция ИКС для предусмотренных сертификатом систем и конфигураций
ИСПДн	Информационная система персональных данных
КИИ	Критическая информационная инфраструктура
Кластер	Два узла ИКС, один из которых может принять работу при отказе другого
LDAP	Протокол доступа к службе каталогов пользователей и групп
Межсетевой экран	Средство, которое разрешает или блокирует сетевые соединения по правилам
NGFW	Межсетевой экран нового поколения с углублённым анализом трафика и дополнительными функциями защиты
ПАК	Программно-аппаратный комплекс: ИКС вместе с подобранной аппаратной платформой
Пресейл-инженер	Технический специалист, который помогает подтвердить требования и подобрать конфигурацию до продажи
Прокси-сервер	Посредник между пользователем и интернет-ресурсом, применяющий правила и ведущий учёт обращений
SIEM	Система централизованного сбора и анализа событий безопасности
Syslog	Распространённый формат и способ передачи журналов событий



Термин	Простое объяснение
Trial	Пробная лицензия для тестирования продукта
VPN	Защищённое соединение пользователя или сети через интернет
IDS	Режим обнаружения признаков сетевых атак
IPS	Режим обнаружения и блокирования трафика по правилам атак
Garnet Web Filter	Дополнительный модуль категоризации сайтов
Suricata	Механизм IDS/IPS, использующий правила для поиска признаков атак
ФСТЭК России	Регулятор в области технической защиты информации; выдаёт сертификаты соответствия средств защиты

13. Контроль знаний партнёра

13.1 Тест по продукту

13.1.1 Вопросы с одним правильным ответом

1. Где обычно устанавливается ИКС? А. Только на рабочих станциях; В. На границе сетей или между сегментами; С. Только на почтовом сервере; D. В SIEM.
2. Что определяет выбор NGFW ИКС или ИКС ФСТЭК? А. Только число сотрудников; В. Только отрасль; С. Требования конкретной системы и проектной документации; D. Наличие филиалов.
3. Что означает ПАК? А. Только лицензия; В. ИКС вместе с аппаратной платформой; С. Услуга аудита; D. База правил IDS/IPS.
4. По какому параметру в первую очередь лицензируется ИКС? А. Число офисов; В. Число пользователей; С. Число сайтов; D. Объём диска.
5. Что делает Garnet Web Filter? А. Создаёт VPN; В. Категоризирует сайты; С. Резервирует питание; D. Управляет телефонией.
6. Чем IPS отличается от IDS? А. IPS может блокировать трафик по правилам; В. IDS работает только с почтой; С. IDS заменяет антивирус; D. Разницы нет.
7. Заменяет ли потоковый антивирус защиту рабочих станций? А. Да; В. Нет, это дополнительный уровень; С. Только в ИКС ФСТЭК; D. Только при VPN.
8. Когда встроенный VPN ИКС нельзя выдавать за сертифицированное средство криптографической защиты? А. Всегда можно; В. Когда проект требует сертификат ФСБ; С. Только для малого бизнеса; D. При наличии AD.
9. Что нужно сделать перед обещанием производительности? А. Ориентироваться только на число сотрудников; В. Проверить каналы, функции, нагрузку и платформу; С. Назвать максимум из буклета; D. Предложить скидку.
10. Что доступно партнёру в проектах от 100 пользователей? А. Автоматическая скидка 50%; В. Пресейл-инженер вендора, ВКС и тестирование; С. Бесплатное оборудование; D. Сертификат ФСБ.
11. Что является правильным итогом первого звонка? А. Рассказать обо всех модулях; В. Договориться о конкретном следующем действии; С. Сразу выставить счёт; D. Пообещать соответствие.
12. Что означает срок реакции поддержки? А. Срок полного исправления; В. Время первоначального ответа; С. Срок поставки; D. Срок лицензии.

13.1.2 Вопросы с несколькими правильными ответами

13. Какие данные нужны для подбора: количество пользователей; скорость каналов; функции; требования к сертификации; любимый браузер директора?
14. Что влияет на производительность: IDS/IPS; антивирусная проверка; число соединений; скорость каналов; цвет корпуса?
15. Что нельзя обещать без проверки: производительность; наличие функции; полное соответствие всем требованиям; скидку; дату рождения разработчика?

16. Какие задачи решает мониторинг: анализ событий; поиск причин проблем; контроль трафика; автоматическое выполнение всех требований закона?
17. Что следует подготовить к тестированию: цель; сценарии; стенд; критерии успеха; ответственных?
18. Что не входит в постоянную работу техподдержки: администрирование сети заказчика; настройка стороннего оборудования; постоянное управление ИКС вместо администратора?

13.1.3 Открытые вопросы

19. Объясните разницу между редакцией продукта и вариантом поставки.
20. Назовите пять признаков потенциальной потребности в ИКС.
21. Какие сведения необходимо приложить к техническому обращению?
22. Почему наличие персональных данных не означает автоматическую необходимость ИКС ФСТЭК?
23. Как партнёру объяснить ценность ИКС без перечисления всех функций?
24. Какие риски снижает отказоустойчивая конфигурация и чего она не резервирует?

13.2 Проверка навыков подбора решения

Для каждого кейса укажите: дополнительные вопросы, редакцию, вариант поставки, модули, необходимость пресейла/ВКС/тестирования и риски неподтверждённых обещаний.

1. Коммерческая компания, 80 пользователей, канал 300 Мбит/с, есть виртуальная среда, нужна фильтрация сайтов, сертификат не требуется.
2. Государственное учреждение, 180 пользователей, проектом предусмотрен сертифицированный межсетевой экран, требуется поставка оборудования.
3. Производственная компания, 450 пользователей, два канала, IDS/IPS и антивирус, простой недопустим, есть несколько сегментов сети.
4. Сеть филиалов, 130 пользователей, требуется связать площадки; заказчик требует «сертифицированное шифрование».
5. Школа, 95 пользователей сейчас и рост до 120, нужен контроль категорий сайтов; заказчик просит показать интерфейс и проверить правила на пилоте.

14. Ответы к контролю знаний

14.1 Ответы к тесту

- 1 — В; 2 — С; 3 — В; 4 — В; 5 — В; 6 — А; 7 — В; 8 — В; 9 — В; 10 — В; 11 — В; 12 — В.
13. Количество пользователей, скорость каналов, функции, требования к сертификации.
 14. IDS/IPS, антивирусная проверка, число соединений, скорость каналов.
 15. Производительность, наличие функции, полное соответствие всем требованиям, скидку.
 16. Анализ событий, поиск причин проблем, контроль трафика.
 17. Цель, сценарии, стенд, критерии успеха, ответственные.
 18. Все перечисленные действия.
 19. Редакция определяет назначение и наличие сертификации; вариант поставки — где и на какой платформе работает ИКС.
 20. Например: замена зарубежного решения, недовольство стоимостью или поддержкой, рост сети, новые филиалы, необходимость фильтрации, сегментации, резервирования или сертифицированного средства.
 21. Организация и контакт, версия ИКС, описание и время проблемы, шаги воспроизведения, ожидаемый и фактический результат, выполненные действия, скриншоты и журналы.
 22. Требования зависят от типа системы, уровня/класса защищённости, модели угроз, технического задания и проекта защиты.
 23. Связать подтверждённую задачу заказчика с результатом: защита сети, контроль доступа, снижение простоев, выполнение требований или удобство сопровождения.
 24. Кластер снижает риск простоя при отказе одного узла ИКС, но не заменяет резервирование питания, каналов связи и сетевого оборудования.

14.2 Ответы к проверке навыков

1. NGFW ИКС, программная поставка в виртуальной среде, Garnet Web Filter. Уточнить одновременную нагрузку, интерфейсы, рост и другие функции. Проект менее 100 пользователей: техническое подключение вендора не заявлять как стандартную возможность без согласования.
2. ИКС ФСТЭК и сертифицированный ПАК в конфигурации проекта. Уточнить тип системы, требования ТЗ, интерфейсы, каналы и функции. Подключить пресейл-инженера, провести ВКС; тестирование — при наличии цели и стенда.
3. NGFW ИКС, если сертификат не требуется; два сопоставимых узла и нужные модули. Обязателен технический расчёт, схема кластера и проверка платформ. Подключить пресейл и предложить тестирование по согласованным сценариям.
4. Сначала уточнить нормативное основание требования. Встроенный VPN ИКС не имеет сертификата ФСБ; при требовании сертифицированной криптографии нужно отдельное средство. Проект от 100 пользователей — подключить пресейл-инженера и проверить схему интеграции.



5. Лицензию подбирать с учётом роста до 120 пользователей; NGFW ИКС и Garnet Web Filter, если сертификат не требуется. Проект переходит порог 100 пользователей: возможны ВКС и тестирование. Зафиксировать категории, сценарии и критерии успешного пилота.