

Анализ раздела

<https://example-security.test/solutions/securelink/>

Демонстрационный пример. Все названия, URL, факты и числовые показатели вымышлены и используются только для иллюстрации методики.

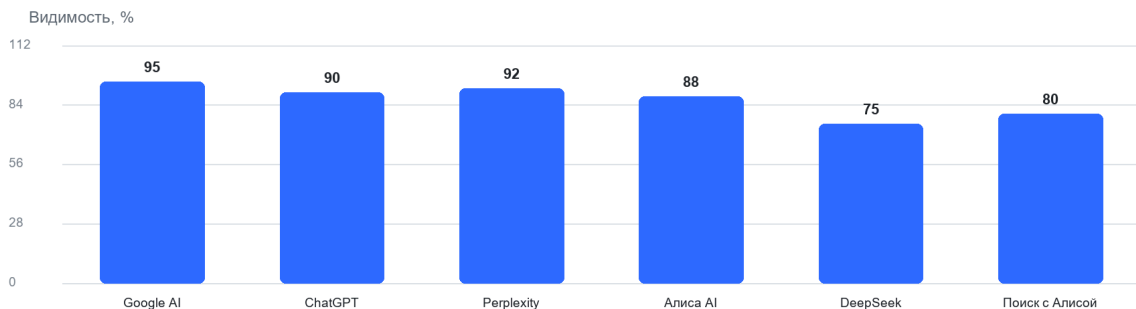
Для анализа были подобраны брендовые промпты: демонстрационная таблица (данные обезличены)

не брендовые промпты: демонстрационная таблица (данные обезличены)

Анализ GEO-видимости

Анализ общей видимости бренда по брендовым промптам

Брендовая GEO-видимость — демонстрационные данные

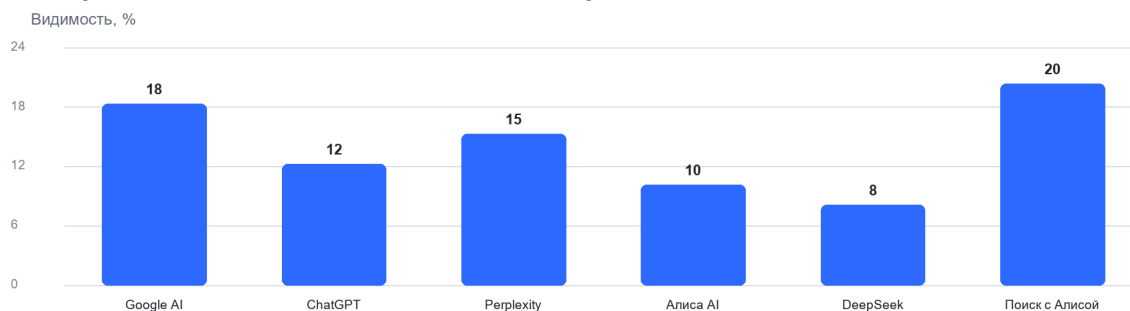


По брендовым промптам SECURELINK показывает высокую видимость: общий показатель составляет около 87%. Продукт устойчиво распознаётся AI-системами как отдельная брендовая сущность, но покрытие различается по платформам.

Максимальная видимость зафиксирована в Google AI Overview — 95%, Perplexity — 92% и ChatGPT — 90%. Алиса AI показывает 88%, Поиск с Алисой — 80%, DeepSeek — 75%. Общий результат высокий, но отдельные платформы требуют дополнительного усиления.

Анализ общей видимости бренда по не брендовым промптам

Небрендовая GEO-видимость — демонстрационные данные

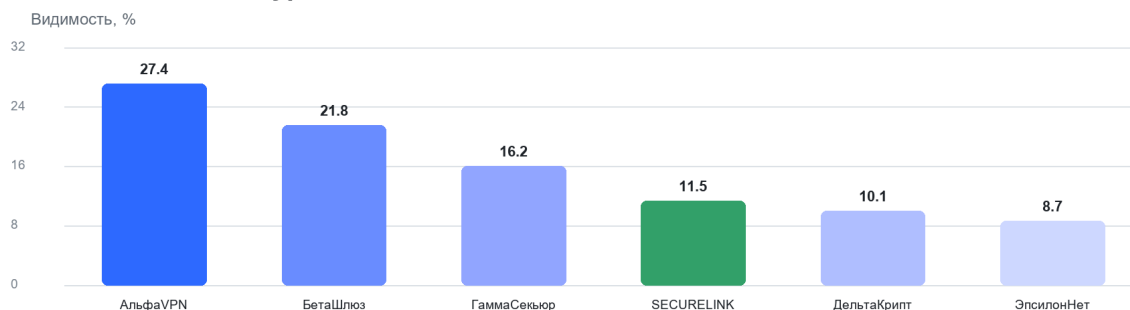


По небрендовым промптам SECURELINK показывает ограниченную видимость: общий показатель составляет около 14%. Это заметно ниже брендового кластера, значит продукт пока недостаточно закреплён в AI-выдаче по категорийным запросам.

Лучший результат даёт Поиск с Алисой — 20%. В Google AI Overview видимость составляет 18%, в Perplexity — 15%, в ChatGPT — 12%, в Алисе AI — 10%, в DeepSeek — 8%. Продукт появляется во всех системах, но пока нерегулярно.

Анализ в разрезе конкурентов

Видимость в конкурентной выдаче



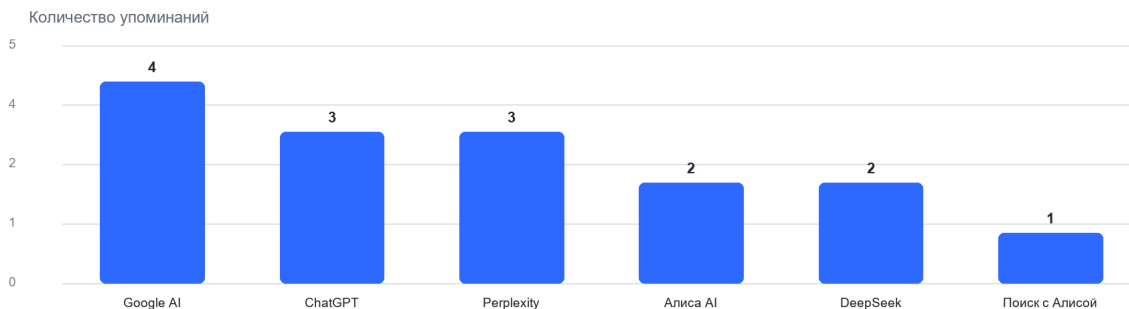
В конкурентной выдаче SECURELINK имеет видимость 11,5% и занимает четвёртое место среди демонстрационных решений сегмента защищённого удалённого доступа и криптографических VPN.

Лидируют АльфаVPN — 27,4% и БетаШлюз — 21,8%. Далее идут ГаммаСекьюр — 16,2%, SECURELINK — 11,5%, ДельтаКрипт — 10,1% и ЭпсилонНет — 8,7%. Отрыв от лидеров указывает на потенциал роста категорийной узнаваемости.

При этом тональность у всех решений положительная, включая SECURELINK. Значит, проблема не в репутации, а в слабой частоте упоминаний и недостаточной связке продукта с небрендовыми категориями: **ГОСТ VPN, криптографический шлюз, защита каналов связи, защищенный удаленный доступ, IPsec/IKEv2, защита распределенной сети, СКЗИ, импортозамещение зарубежная VPN-платформа А.**

Анализ упоминаний бренда

Упоминания SECURELINK по AI-системам



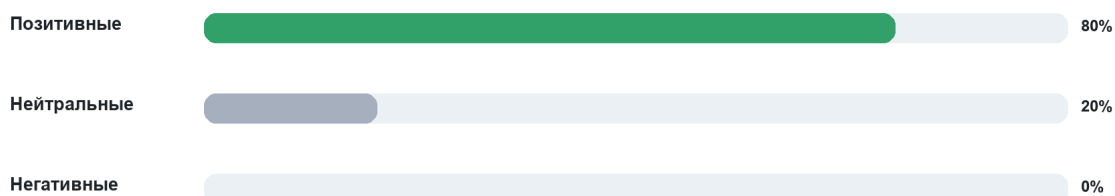
По блоку упоминаний SECURELINK набирает 15 упоминаний. Это подтверждает, что продукт присутствует в небрендовой AI-выдаче, но пока появляется точно и не закреплён как один из основных ответов по теме защищённых каналов связи и корпоративного VPN.

Основной вклад дают Google AI Overview — 4 упоминания, ChatGPT и Perplexity — по 3. Алиса AI и DeepSeek дают по 2 упоминания, Поиск с Алисой — 1. Распределение показывает, где стоит усиливать источниковое присутствие.

Рекомендация: для роста нужно усиливать присутствие SECURELINK в экспертных и справочных материалах под запросы: **ГОСТ VPN, криптографический шлюз, защита каналов связи, защищенный удаленный доступ, IPsec VPN, IKEv2, СКЗИ, защита каналов связи для КИИ, импортозамещение зарубежная VPN-платформа А / зарубежная платформа В / зарубежная платформа С.**

Тональность упоминаний

Тональность упоминаний — демонстрационные данные

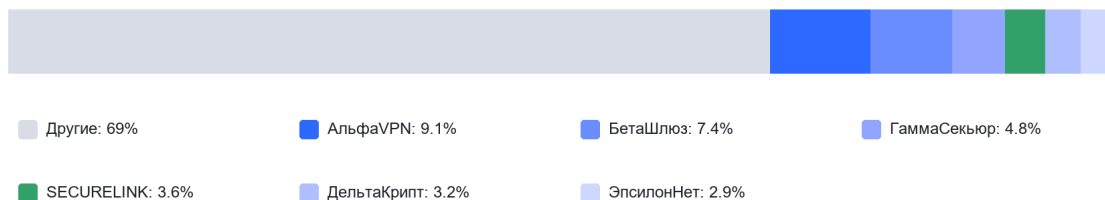


Тональность упоминаний SECURELINK в целом положительная: 80% упоминаний позитивные, 20% — нейтральные. Негативных упоминаний в демонстрационной выборке нет.

Это хороший репутационный сигнал для GEO: когда продукт появляется в ответах нейросетей, он описывается в благоприятном или нейтральном контексте. Основная проблема не в тональности, а в низкой частоте появления по небрендовым промптам.

Доля голосов (Share of Voice)

Share of Voice — демонстрационные данные



По Share of Voice SECURELINK занимает 3,6%. Продукт присутствует в конкурентном поле, но пока уступает основным игрокам категории защищённых каналов связи и корпоративных VPN-решений.

Лидируют АльфаVPN — 9,1% и БетаШлюз — 7,4%. Далее идут ГаммаСекьюр — 4,8%, SECURELINK — 3,6%, ДельтаКрипт — 3,2% и ЭпсилонНет — 2,9%. От лидеров продукт отстаёт примерно в 2–2,5 раза.

При этом доля «Другие» составляет 69%, то есть выдача сильно фрагментирована. Для роста доли голоса нужно усиливать присутствие продукта в сравнительных и экспертных контекстах: **ГОСТ VPN, криптографический шлюз, защищенный удаленный доступ, защита каналов связи для КИИ, IPsec/IKEv2, СКЗИ, импортозамещение зарубежная VPN-платформа А, сравнение с АльфаVPN, БетаШлюз, ЭпсилонНет и ДельтаКрипт.**

Анализ выдачи по брендовым промптам

Данные по выдаче сведены в таблицу: демонстрационная таблица (данные обезличены)

Частотность в примере основана на синтетической демонстрационной выборке

По брендовым промптам SECURELINK упоминается в 26 ответах из 30 проверок. В целом брендовая видимость сильная: продукт стабильно распознается Google AI Overview, ChatGPT, Perplexity и Алисой AI (GPT). Основная просадка связана с Поиском с Алисой, где ответы по этим промптам не сформированы.

По нейросетям: **Google AI Overview, ChatGPT, Perplexity и Алиса AI (GPT)** упоминают бренд по всем 5 промптам. **Google AI Overview, ChatGPT и Perplexity упоминают SECURELINK по всем 5 промптам; Алиса AI и DeepSeek — по 4 из 5, Поиск с Алисой — по 3 из 5.**

Дополнительно официальный сайт example-security.test используется как источник в 9 случаях из 30. Источниковые упоминания дают **Google AI Overview и Perplexity**; остальные нейросети бренд называют, но официальный сайт в источниках не показывают.

Анализ выдачи по не брендовым промптам

Таблица с анализом: демонстрационная таблица (данные обезличены)

Частотность в примере основана на синтетической демонстрационной выборке

По небрендовым промптам SECURELINK упоминается в 15 ответах из 120 проверок. Видимость низкая: продукт пока слабо закреплен в ИИ-выдаче по ключевым категориям **защиты каналов связи, ГОСТ VPN, криптографических шлюзов, IPsec/IKEv2 и защищенного удаленного доступа.**

Лучший результат у запроса **“отечественная система защиты каналов связи”** — 3 из 6. Частично продукт появляется по запросам **“аппаратно-программный криптошлюз”, “VPN с ГОСТ шифрованием”, “IKEv2 VPN с российской криптографией”, “импортозамещение зарубежная VPN-платформа А” и “аналог зарубежная платформа А зарубежная платформа В зарубежная платформа С для защиты каналов связи”.**

Основная проблема — нулевая видимость по базовым высокочастотным и категорийным интендам: **защита каналов связи, защищенный удаленный доступ, защищенная передача данных по сети, криптографический шлюз, ГОСТ VPN для организации, IPsec VPN для корпоративной сети, защита удаленных рабочих мест, защита каналов связи для КИИ.**

По нейросетям распределение слабое и равномерно низкое: **Поиск с Алисой, Google AI Overview и Perplexity** дали по 2 упоминания, **ChatGPT, Алиса AI (GPT) и DeepSeek** — по 1. Официальный сайт example-security.test используется как источник в 22 случаях из 120, что также ограничивает GEO-эффект.

Рекомендации по подготовке/доработке контента

По брендовым запросам сайт или упоминание бренда встречается 5 и более раз из 6: демонстрационная таблица (данные обезличены)

В данном случае доработки не требуются.

По не брендовым запросам данные представлены в таблице: демонстрационная таблица (данные обезличены)

Ниже указаны рекомендации для запросов, которые встречаются менее чем в 3х нейросетях из 6:

Промпт	Частотность	Упоминания	Приоритет	Целевая страница	Рекомендация
защита каналов связи	720	0 из 6	Высокий	https://example-security.test/knowledge/6735/	Доработать статью как основной материал под интент “защита каналов связи”: добавить answer-first-блок, виды защиты, ГОСТ VPN, IPsec/IKEv2 и прямую связку с АПК “SECURELINK”.
защищенный удаленный доступ	260	0 из 6	Высокий	https://example-security.test/knowledge/6850/	Усилить блок “защищенный удаленный доступ”: VPN, MFA, IPsec, ГОСТ-шифрование, доступ сотрудников и администраторов к корпоративной сети.
защищенная передача данных по сети	680	0 из 6	Высокий	https://example-security.test/knowledge/6735/	Добавить отдельный раздел про защищенную передачу данных: шифрование канала, целостность, аутентификация сторон, защита трафика между филиалами.

криптографический шлюз	140	0 из 6	Высокий	Новая статья	Подготовить отдельный материал "Криптографический шлюз: что это такое и как защищает каналы связи". Внутри связать класс решений с АПК "SECURELINK".
аппаратно-программный криптошлюз	24	1 из 6	Средний	Новая статья	Сделать отдельную статью или раздел про АПК-криптошлюзы: отличие от программного VPN, роль СКЗИ, IPsec/IKEv2, ГОСТ-алгоритмы и сценарии для КИИ/ГИС.
VPN с ГОСТ шифрованием	9	1 из 6	Средний	https://example-security.test/knowledge/6660/	Доработать статью про VPN: добавить блок "VPN с ГОСТ-шифрованием", отличие от обычного VPN и применение в корпоративной инфраструктуре.
ГОСТ VPN для организации	3	0 из 6	Средний	https://example-security.test/knowledge/6660/	Вынести точную формулировку в Н2/Н3, добавить сценарии для организаций: филиалы, удаленные сотрудники, ГИС, КИИ, защищенные каналы связи.
IPsec VPN для корпоративной сети	1	0 из 6	Средний	https://example-security.test/knowledge/6561/	Усилить статью под "IPsec VPN для корпоративной сети": туннельный режим, связь филиалов, удаленный доступ и применение АПК "SECURELINK".

IKEv2 VPN с российской криптографией	—	1 из 6	Средний	https://example-security.test/knowledge/6561/	Добавить блок про IKEv2 в российских VPN-решениях: обмен ключами, IPsec, ГОСТ-алгоритмы, сертифицированные СКЗИ.
шифрование трафика IPsec	4	0 из 6	Средний	https://example-security.test/knowledge/6561/	Расширить раздел про IPsec: что именно шифруется, транспортный и туннельный режимы, защита трафика между узлами.
межсетевой экран с криптографической защитой	7	0 из 6	Средний	https://example-security.test/knowledge/6864/	Добавить сравнение NGFW и криптографической защиты: экран фильтрует трафик, а криптографический шлюз шифрует канал.
защита удаленных рабочих мест	99	0 из 6	Высокий	https://example-security.test/knowledge/6850/	Добавить сценарии защиты удаленных рабочих мест: VPN-подключение, MFA, доступ к корпоративной сети, контроль политик безопасности.
защищенное подключение филиалов	—	0 из 6	Средний	https://example-security.test/knowledge/6735/	Добавить блок про site-to-site VPN и защищенное подключение филиалов через IPsec/ГОСТ VPN.

защита распределенной корпоративной сети	—	0 из 6	Средний	https://example-security.test/knowledge/6891/	Доработать статью про методы защиты сетей: добавить отдельный сценарий для распределенных сетей, филиалов и удаленных площадок.
безопасный доступ к ГИС	7	0 из 6	Средний	https://example-security.test/knowledge/6888/	Добавить раздел про доступ к ГИС: требования регуляторов, СКЗИ, защищенный канал, ГОСТ-шифрование.
защита каналов связи для КИИ	—	0 из 6	Высокий	https://example-security.test/knowledge/6735/	Усилить блок про КИИ: требования к защищенным каналам, сертифицированные СКЗИ, IPsec, ГОСТ VPN, сценарии для критической инфраструктуры.
импортозамещение зарубежная VPN-платформа А	—	1 из 6	Высокий	Новая статья	Подготовить статью "Импортозамещение зарубежная VPN-платформа А: российские решения для защиты каналов связи". Упомянуть АльфаVPN, БетаШлюз, ЭпсилонНет и АПК "SECURELINK".
русская система защищенного удаленного доступа	—	0 из 6	Высокий	https://example-security.test/knowledge/6850/	Добавить блок про российские решения для защищенного удаленного доступа: ГОСТ VPN, IPsec, сертификация, сценарии для бизнеса и госсектора.

аналог зарубежная платформа А зарубежная платформа В зарубежная платформа С для защиты каналов связи	—	2 из 6	Высокий	Новая статья	Подготовить сравнительный материал про российские альтернативы зарубежным VPN/NGFW-реше ниям для защиты каналов связи.
--	---	--------	---------	--------------	--

Анализ оптимизации страницы под GEO

Страница [«SECURELINK»](#) уже имеет хорошую базу для продвижения в GEO, так как на ней достаточно четко раскрыты назначение продукта, технологическая основа и сценарии применения. В первом экране продукт позиционируется как решение для профессиональной защиты каналов связи и удаленного доступа, а ниже дополнительно поясняется, что SECURELINK предназначена для защищенной передачи данных по сети и построена на шифровании трафика по IPsec и распределенных межсетевых экранах. Для нейросетей это важный плюс: страница не ограничивается брендом, а связывает продукт с конкретными задачами и технологиями.

Сильная сторона страницы — наличие большого количества сущностей, которые хорошо считываются AI-системами: ГОСТ-криптография, IPsec, IKEv2, СКЗИ, межсетевой экран, защищенный удаленный доступ, защита каналов связи, ГИС, КИИ, профильные регуляторные требования, централизованное управление, криптошлюз, удаленные рабочие места, филиальная сеть. Также хорошо раскрыта продуктовая линейка: [SECURELINK-Управление](#), аппаратные криптошлюзы [АПК SECURELINK](#), [SECURELINK-Клиент](#), [SECURELINK-Офис](#), [SECURELINK-TK](#). Это помогает нейросетям точнее понимать не только сам бренд, но и состав решения.

Также положительно влияет наличие проверяемых фактов: 12+ лет экспертизы, управление 2 500+ устройств из одной точки, снижение ТСО на 8–12%, отказы оборудования менее 2% в год, гарантия до пяти лет, подтвержденное соответствие профильным требованиям, классы требуемые классы СКЗИ, возможность защиты ГИС требуемого класса, ИСПДн требуемого уровня защищенности и значимых объектов значимых объектов КИИ. Такие факты стоит отдельно вынести в блок “Факты о SECURELINK”, потому что нейросетям проще извлекать и цитировать структурированную информацию.

Основное ограничение страницы — недостаточная ориентация на небрендовые информационные запросы. Сейчас материал хорошо описывает продукт, но не всегда прямо отвечает на формулировки вроде “что такое ГОСТ VPN”, “что такое криптографический шлюз”, “чем IPsec VPN отличается от обычного VPN”, “какое решение выбрать для защиты каналов связи”, “чем заменить зарубежная VPN-платформа А”, “какое российское решение подходит для защищенного удаленного доступа”. Для GEO важно добавить answer-first блоки, где SECURELINK будет явно связана с этими классами и задачами.

Для усиления страницы стоит добавить блок “Коротко о продукте” в табличном формате: класс решения, задачи, технологии, для кого подходит, регуляторика, компоненты, сценарии применения, альтернативы/замена. Также нужен FAQPage с вопросами про ГОСТ VPN, IPsec/IKEv2, криптошлюз, СКЗИ, защиту каналов связи, КИИ/ГИС, импортозамещение зарубежная VPN-платформа А/зарубежная платформа В/зарубежная платформа С. Отдельно стоит добавить нейтральный сравнительный блок “SECURELINK, АльфаVPN, БетаШлюз, ЭпсилонНет: в каких задачах применяются решения для защиты каналов связи”, чтобы страница чаще попадала в AI-ответы по сравнительным и рекомендательным промптам.

Анализ внутренней перелинковки

Данные о внутренней перелинковке представлены в таблице: демонстрационная таблица (данные обезличены)

На страницу ведет очень большая внутренняя ссылочная масса: найдено 860 строка со ссылкой на </solutions/securelink/>. Источники разнообразные: главная, продуктовые разделы, страницы услуг, новости, вебинары, страницы документов и блоговые материалы.

Анкор-лист в целом релевантный: чаще всего используются брендово-описательные анкеры “АПК «SECURELINK»”, “АПК «SECURELINK» Защита каналов связи и удаленного доступа”, “АПК «SECURELINK» Профессиональная защита каналов связи и удаленного доступа от соавторов IPsec”. Это помогает закреплять за страницей связь с продуктом, IPsec и задачей защиты каналов связи.

Главный минус для GEO — однотипность анкорного профиля. Анкор “«SECURELINK» Российский ГОСТ VPN и IPsec-защита каналов связи” встречается только 1 раз, “Solar SECURELINK” — 15 раз, “Подробнее” — 3 раза. То есть небрендовые сущности почти не используются как самостоятельные анкорные сигналы.

Рекомендация: усилить контентную перелинковку из статей про VPN, IPsec/IKEv2, шифрование каналов связи, защиту удаленного доступа, ГИС/КИИ и импортозамещение. В анкорах чаще использовать формулировки: “ГОСТ VPN для организации”, “криптографический шлюз”, “IPsec VPN для корпоративной сети”, “защита каналов связи для КИИ”, “защищенный удаленный доступ”, “российское решение для защиты каналов связи”.

Анализ внешних ссылок

Выгрузка данных по внешним ссылкам: демонстрационная таблица (данные обезличены)

Найдено 24 внешние ссылки на страницы раздела SECURELINK. Из них 14 помечены как низкокачественные или nofollow, в основном это BHS/SEO-доноры с нерелевантными анкерами. Часть таких ссылок уже имеет статус [removedfromhtml](#).

Полезных контентных упоминаний — 10: отраслевой обзор решения SECURELINK, партнёрский кейс внедрения и несколько тематических материалов с релевантными анкерами. Это хорошие по смыслу ссылки, потому что рядом с брендом появляются важные GEO-сущности: криптозащита каналов связи, регуляторные требования, IPsec/IKEv2.

Сейчас внешняя ссылочная масса не формирует устойчивую экспертную ассоциацию “SECURELINK = российский ГОСТ VPN / IPsec-криптошлюз / защита каналов связи”. Для AI-выдачи этого мало: нейросетям нужны не просто ссылки, а контекстные упоминания в релевантных материалах.

Рекомендация: развивать экспертные публикации в ИБ-СМИ, партнерских блогах и каталогах решений: обзоры ГОСТ VPN, сравнения российских средств защиты каналов связи, материалы про IPsec/IKEv2, КИИ, ГИС, импортозамещение зарубежная VPN-платформа А/зарубежная платформа В/зарубежная платформа С. Важно, чтобы рядом со ссылкой прямо раскрывалось, что SECURELINK — это российское решение для защиты каналов связи и удаленного доступа на базе ГОСТ-криптографии и IPsec.

Пул рекомендаций

1. Добавить GEO-блок в первый экран

SECURELINK — российское решение для защиты каналов связи и защищенного удаленного доступа на базе ГОСТ-криптографии, IPsec/IKEv2 и распределенных межсетевых экранов. Продукт подходит крупным организациям, госсектору, компаниям с филиальной сетью, удаленными рабочими местами, ГИС, ИСПДн и объектами КИИ, где требуется сертифицированная защита трафика и централизованное управление криптографической инфраструктурой.

2. Сделать блок “Коротко о продукте”

В формате таблицы:

Класс: ГОСТ VPN / IPsec VPN / криптографический шлюз / СКЗИ

Задачи: защита каналов связи, защищенный удаленный доступ, шифрование трафика, подключение филиалов, защита ГИС и КИИ

Для кого: enterprise, госсектор, банки, промышленность, распределенные компании, организации с КИИ

Технологии: ГОСТ-криптография, IPsec, IKEv2, межсетевой экран, централизованное управление

Компоненты: SECURELINK-Управление, АПК SECURELINK, SECURELINK-Клиент, SECURELINK-Офис, SECURELINK-ТК

Сертификация: профильные регуляторные требования, требуемые классы СКЗИ, МЭ 4 класса

Альтернативы/замена: АльфаVPN, БетаШлюз, ЭпсилонНет, зарубежная VPN-платформа А, зарубежная платформа В, зарубежная платформа С

3. Добавить FAQPage

Минимальный набор FAQ:

Что такое SECURELINK?

Что такое ГОСТ VPN?

Что такое криптографический шлюз?

Чем IPsec VPN отличается от обычного VPN?

Для каких компаний подходит SECURELINK?

Подходит ли SECURELINK для защищенного удаленного доступа?

Можно ли использовать SECURELINK для защиты каналов связи КИИ?

Можно ли использовать SECURELINK для безопасного доступа к ГИС?

Какие компоненты входят в линейку SECURELINK?

Какие сертификаты профильных регуляторных требований есть у решения?

Можно ли использовать SECURELINK для импортозамещения зарубежная VPN-платформа А?

4. Усилить блок про ГОСТ VPN и криптографические шлюзы

Сделать отдельный SEO/GEO-раздел “SECURELINK как ГОСТ VPN и криптографический шлюз”. Сейчас эти сущности есть на странице, но они не раскрыты как самостоятельный объясняющий блок. Нужна нейтральная формулировка: ГОСТ VPN обеспечивает защищенный канал связи с использованием российских криптоалгоритмов, IPsec/IKEv2 отвечает за построение защищенного туннеля, а

криптографический шлюз шифрует трафик между филиалами, дата-центрами, удаленными рабочими местами и корпоративными ресурсами.

5. Добавить entity-rich формулировки

На странице должны явно встречаться синонимы и сущности:

ГОСТ VPN

IPsec VPN

IKEv2 VPN

криптографический шлюз

аппаратно-программный криптошлюз

СКЗИ

защита каналов связи

защищенный удаленный доступ

шифрование трафика IPsec

защищенное подключение филиалов

защита распределенной корпоративной сети

защита каналов связи для КИИ

безопасный доступ к ГИС

российское решение для защиты каналов связи

импортозамещение зарубежная VPN-платформа А

аналог зарубежная VPN-платформа А / зарубежная платформа В / зарубежная платформа С

6. Сделать факты проверяемыми

Все сильные заявления стоит сопровождать конкретикой и вынести в отдельный блок “Факты о SECURELINK”:

12+ лет экспертизы в защите каналов связи

снижение ТСО на 8–12%

управление 2 500+ устройств из одной точки

отказы оборудования менее 2% в год

гарантия до 5 лет

подтверждённое соответствие профильным требованиям

требуемые классы СКЗИ

межсетевой экран 4 класса типа А

защита ГИС требуемого класса

защита ИСПДн требуемого уровня защищённости

защита значимых объектов значимых объектов КИИ

7. Добавить Schema.org

Рекомендуемый минимум:

SoftwareApplication или Product

Organization

FAQPage

BreadcrumbList

WebPage

ItemList для компонентов и преимуществ

DefinedTermSet для терминов ГОСТ VPN / IPsec / IKEv2 / СКЗИ / криптографический шлюз

ProductModel для компонентов SECURELINK-Управление, АПК SECURELINK, SECURELINK-Клиент, SECURELINK-Офис, SECURELINK-ТК

8. Усилить контентный кластер под слабые небрендовые промпты

Нужно доработать материалы под запросы, где продукт сейчас почти не появляется в нейросетях: защита каналов связи, защищенный удаленный доступ, защищенная передача данных по сети, криптографический шлюз, ГОСТ VPN для организации, IPsec VPN для корпоративной сети, защита удаленных рабочих мест, защита каналов связи для КИИ, импортозамещение зарубежная VPN-платформа А, российская система защищенного удаленного доступа.

9. Создать новые материалы

В первую очередь нужны статьи:

“Криптографический шлюз: что это такое и как защищает каналы связи”

“Аппаратно-программный криптошлюз: отличие от программного VPN”

“Импортозамещение зарубежная VPN-платформа А: российские решения для защиты каналов связи”

“Российские аналоги зарубежная платформа А, зарубежная платформа В и зарубежная платформа С для защиты каналов связи”

“ГОСТ VPN для организации: как выбрать решение для филиалов, КИИ и удаленного доступа”

10. Усилить внутреннюю перелинковку

Из тематически близких материалов: статей про VPN, ГОСТ VPN, IPsec/IKEv2, шифрование каналов связи, защищенный удаленный доступ, КИИ, ГИС, филиальные сети и импортозамещение зарубежная VPN-платформа А. В анкерах стоит чаще использовать не только бренд, но и запросные формулировки: ГОСТ VPN для организации, криптографический шлюз, IPsec VPN для корпоративной сети, защита каналов связи для КИИ, защищенный удаленный доступ, российское решение для защиты каналов связи.

11. Усилить внешние ссылки

Для роста GEO-эффекта лучше развивать не массовые ссылки, а экспертные упоминания: обзоры российских ГОСТ VPN, материалы про защиту каналов связи, IPsec/IKEv2, КИИ, ГИС, импортозамещение зарубежная VPN-платформа А, публикации в ИБ-СМИ, партнерские страницы интеграторов и кейсы внедрения.