



ТОМСКЭНЕРГОСБЫТ

Открытое акционерное общество «Томская энергосбытовая компания»

УТВЕРЖДАЮ

Председатель закупочной комиссии

ОАО «ТомскэнергоСбыт»

А.В. Булгаков

Техническое задание на проведение закупки услуг

Основание для проведения: ГКПЗ 424.14.00005 Приобретение средств защиты информации

Наименование закупки: приобретение системы защиты сетевой инфраструктуры Компании.

Начальная (предельная) стоимость оказываемых услуг 5 128 000 (пять миллионов сто двадцать восемь тысяч) рублей без учёта НДС.

Техническое задание на приобретение системы защиты сетевой инфраструктуры Компании

1. Общие требования:

- 1.1. Исполнитель обязуется поставить средства защиты (далее – оборудование) и выполнить работы по созданию защищенной информационной системы передачи данных для Заказчика.
- 1.2. Работы, предоставляемые в соответствии с п.п. 1.1 настоящего технического задания должны оказываться в полном объеме и с надлежащим качеством. Исполнитель несет ответственность за качество выполнения работ, за соблюдение пожарной безопасности и правил техники безопасности.
- 1.3. Предоставляемое Исполнителем оборудование должно отвечать требованиям нормативно-технических документов и стандартов, действующих на территории Российской Федерации.
- 1.4. Предоставляемое оборудование должно интегрироваться в существующую сеть IP.
- 1.5. Обязательным является предоставление Исполнителем годовой круглосуточной службы клиентской поддержки;
- 1.6. Оплата работ осуществляется в форме безналичного расчета путем перечисления денежных средств на расчетный счет Исполнителя в течение 30 календарных дней с даты подписания акта приемки оказанных работ.

2. Требования к оказанию работ:

2.1. Защищенная информационная система передачи данных, должна включать в себя следующие функциональные компоненты (подсистемы):

- подсистему регистрации и учета;
на основе программно-аппаратного решения StoneGate IPS, осуществляющего сбор событий сетевой безопасности и управляющего сервера.
- подсистему межсетевого экранирования;

на основе программного и программно-аппаратного решения продуктов CSP VPN от S-terra, осуществляющего фильтрацию сетевого трафика.

- подсистему анализа защищенности;
на основе программного решения XSpider 7.8, используемого для проверки на возможные уязвимости программного обеспечения и аппаратные платформы.
- подсистему обнаружения вторжений;
на основе программно-аппаратного решения StoneGate IPS, осуществляющего сканирование сетевого трафика и детектирование атак.
- подсистему криптографической защиты открытых каналов связи.
на основе программного и программно-аппаратного решения продуктов CSP VPN от S-terra, осуществляющего шифрование передаваемой информации.

Перечень поставляемого Исполнителем оборудования приведен в Таблице 2.1.1

Технические требования к поставляемому оборудованию, приведены в Приложении 1 к настоящему техническому заданию.

Таблица 2.1.1. Перечень поставляемого оборудования

PN	Описание	Кол-во
G-3000-L-5041-4-RED-KC2 (версия 3.11)	KW Express Lite EL15, Redundant, 4xLAN 1Gb, Rack mount 1U	1
C-X-WIN-KC2 (версия 3.11)	Программный комплекс CSP VPN Client	40
G-1000-L-5007-3-KC2 (версия 3.11)	Kraftway Credo VV20, 3xLAN 1Gb, Rack mount 1U, СПДС- 01-1ГБ	27
kb-sobol	ПАК "Соболь" (версия 3.0), PCI-E - комплект с DS 1992	1
KP-100	Система централизованного управления на 100 лицензий	1
DEV-IPS-1205-C1-R	Аппаратная платформа StoneGate IPS-1205-C1	1
LIC-IPS-1205-C1-R	Право на использование программного обеспечения StoneGate IPS-1205-C1	1
M-APP-IPS-1205-C1	Ключ активации сервиса стандартной технической поддержки и получение обновлений программного обеспечения для StoneGate IPS-1205-C1, сроком на 12 мес.	1
FP-IPS-ANZ5	Право на использование программного обеспечения StoneGate IPS-ANZ5	1
SG-SPO-IPS2	Базовый пакет сертифицированного ПО StoneGate IPS для моделей StoneGate IPS 1060, 1205, 3201 и ПО от 600 до 2000 Мбит/с включительно	1
	Сервер для ПО StoneGate Management Center в составе:	1
7160K2G	Express x3530M4, 1x Xeon E5-2407v2 2.4GHz 10M 4C 1333MHz (80W), 8GB (1x 8GB (2Rx8, 1.35V) 1600MHz LP RDIMM), O/B 3.5" HS SAS/SATA(4), M5110, No Optical, 1x460W HS PSU	1
90Y8826	Express IBM 1TB 7.2K 6Gbps NL SATA 3.5in G2HS HDD	1
90Y8822	Express IBM 2TB 7.2K 6Gbps NL SATA 3.5in G2HS HDD	1
P73-06437-L	Soft Microsoft WinSvrStd2008R2SP1x64Rus1pk1-4CPU5CltLCP зам. P73-05121 (P73-06437-L) lic+id866072	1
P73-06437-D	Soft Microsoft WinSvrStd2008R2SP1x64Rus1pk1-4CPU5CltLCP зам. P73-05121 (P73-06437-D) inst.pk+id86607	1
LIC-SG-SMC-2	StoneGate Management Center License for 2 nodes. A node (either a single unit or a cluster) can be a FW/VPN, a FW, or a VPN gateway, or an IPS sensor. Includes both a Management Server and a Log Server, which can be installed on a single server or on separate servers	1
M-SG-SMC-2	Basic (8/5) Support and Maintenance for SMC-2 15 Months	1
	Сканер безопасности XSpider 7.8	

2.2. Установка и настройка оборудования защищенной информационной системы передачи данных должно производиться по следующим адресам Таблицы 2.2.1.;

Таблица 2.2.1. Адреса установки и настройки оборудования защищенной информационной системы передачи данных

№	Адрес площадки
1	г. Томск, ул. Котовского, 19
2	г. Томск, Иркутский тр-т, 37б
3	г. Томск, просп. Ленина 195
4	с. Мельниково, ул. Московская, 13
5	с. Кривошеино, ул. Ленина, 31
6	с. Кожевниково, ул. Гагарина, 2 стр. 1
7	с. Бакчар, ул. Ленина, 48
8	с. Молчаново, ул. Валикова, 10, стр.1
9	г. Асино, ул. Ленина, 10
10	с. Тегульдэт, ул. Парковая, 5
11	с. Первомайское, ул. Степная, 26
12	с. Зырянское, пер. Энергетический, 5
13	с. Белый Яр. Октябрьская 2а
14	г. Колпашево, ул. Базарная, 44
15	г. Колпашево, ул. Победы, 5
16	г. Стрежевой, 2-ой мкрн., д. 236
17	с. Каргасок, ул. Пушкина, 45
18	с. Парабель, ул.Чехова, 21 В
19	с. Чажемто, ул. Пристанская, 2
20	с. Александровское, ул. Лебедева, 8
21	г. Кедровый. Промзона а/я №1
22	г. Томск, ул. Пушкина, 63 стр. 6
23	г. Томск ул. Герцена, 61/1
24	г. Томск, пр. Фрунзе ,119/5
25	г. Томск, ул. Лазо, 12/3
26	г. Томск, ул. Интернационалистов, 17/1
27	г. Томск, ул. Вавилова, 10
28	п. Кафтанчиково, ул. Коммунистическая 89
29	п. Молодежный, д.145
30	с. Октябрьское, ул. Заводская. 4
31	с. Межениновка, ул. Первомайская.23
32	г. Томск, пос. Зональный ул. Солнечная 19/1
33	г. Асино, пер. Электрический, 3/1, офис 1
34	с. Подгорное, ул. Советская 19
35	г. Томск, Мира 48/3;
36	п. Кисловка, ул. Мира, 12;
37	п. Богашево, ул. Новостройка, 1а;
38	п. Зоркальцево, ул. Совхозная, 14;
39	п. Нелюбино, ул. Дорожная, 3;
40	с. Тогур, ул. Ленина, 10
41	г. Колпашево, ул. Толстого 14
42	с. Александровское, ул. Казахстан 16
43	г. Томск, Нахимова, 8
44	г. Томск, пер. Нечевский, 20а

Должна быть проведена настройка всего поставляемого ПО и оборудования;

2.3. В рамках выполнения работ по созданию защищенной информационной системы передачи данных Исполнителем должны быть выполнены следующие работы:

- а) обследование сетевой инфраструктуры Заказчика. Разработка и согласование с Заказчиком плана реализации проекта с последующей его еженедельной актуализацией;
- б) техническое проектирование защищенной информационной системы передачи

данных;

- в) внедрение защищенной информационной системы передачи данных;
- и) ввод защищенной информационной системы передачи данных в опытную и промышленную эксплуатацию;
- к) предоставление службы клиентской поддержки;
- л) разработка и предоставление документации:
 - пояснительной записки к техническому проекту;
 - рабочей документации для каждого компонента (подсистемы) защищенной информационной системы передачи данных;
 - эксплуатационной документации для каждого компонента (подсистемы) защищенной информационной системы передачи данных.

2.3.1. Обследование сетевой инфраструктуры

Обследование сетевой инфраструктуры Заказчика должно включать в себя:

- а) сбор информации о топологии и физической структуре локальной вычислительной сети объектов Заказчика для дальнейшего проектирования защищенной информационной системы;
- б) определение и описание существующих сегментов сети до и после создания защищенной информационной системы;
- в) определение и описание существующих и необходимых IP-адресов;
- г) определение и описание существующих и необходимых сетевых интерфейсов;
- д) определение и описание существующих и необходимых технологий маршрутизации и коммутации информационных потоков;
- е) составление перечня существующих и необходимых сетевых объектов (подсети, шлюзы, и т.д.);
- и) построение топологии сетевой инфраструктуры защищенной информационной системы передачи данных;

2.3.2. Техническое проектирование

В рамках технического проектирования должна быть выполнена разработка технического проекта и комплекта эксплуатационной документации для создаваемой защищенной информационной системы передачи данных Заказчика.

Технический проект должен включать следующие документы:

2.3.2.1. Пояснительная записка к техническому проекту на создание защищенной информационной системы передачи данных, содержащая техническое решение по внедрению системы, для всех компонентов (подсистем) защиты Заказчика.

2.3.2.2. Спецификация комплекса технических средств защиты.

2.3.3. Внедрение защищенной информационной системы передачи данных

Условием начала работ по внедрению защищенной информационной системы передачи данных должен являться Акт готовности к внедрению, подписанный представителем Заказчика и ответственным представителем Исполнителя.

В рамках работ по внедрению защищенной информационной системы передачи данных должны быть выполнены следующие работы:

- а) настройка компонентов (подсистем) защиты, заключающаяся в следующем:
 - 1) настройка подсистемы регистрации и учета, а также подсистемы обнаружения вторжений, включающая в себя:
 - установку и настройку программного обеспечения системы управления и мониторинга StoneSoft;
 - настройку StoneGate IPS в режиме обнаружения и предотвращения вторжений (режим IPS), после сбора необходимой статистики в режиме обнаружения вторжений (режим IDS);
 - установку и настройку программного обеспечения системы централизованного управления S-terra;
 - 2) настройка подсистем межсетевого экранирования и криптографической защиты открытых каналов связи, включающая в себя настройку программных и программно-аппаратных решений от S-terra;
 - 3) настройка подсистемы анализа защищенности, включающая в себя настройку сканера безопасности XSpider;
- б) пусконаладочные работы, заключающиеся в следующем:
 - 1) настройке IP-адресации на внедряемых средствах защиты и на

существующем сетевом оборудовании Заказчика;

2) настройке сетевых интерфейсов на внедряемых средствах защиты и на существующем сетевом оборудовании Заказчика;

3) настройке маршрутизации и коммутации;

2.3.4. Ввод в опытную и промышленную эксплуатацию

В рамках работ по вводу защищенной информационной системы передачи данных в промышленную эксплуатацию необходимо провести:

а) предварительные испытания;

б) опытную эксплуатацию;

в) приемо-сдаточные испытания, согласно разработанной Исполнителем и согласованной с Заказчиком программы и методики испытаний.

При необходимости по результатам опытной эксплуатации провести корректировку технической и рабочей документации.

2.3.5. Предоставление службы клиентской поддержки

Обязательным является предоставление Исполнителем круглосуточной службы клиентской поддержки, включающей в себя следующие этапы взаимодействия сторон:

Таблица 2.3.5.1. Этапы взаимодействия сторон

№	Этапы взаимодействия	Описание
1	Оперативный прием и фиксирование запросов от Заказчика	Прием и классификация запросов дежурным инженером Исполнителя по телефону, e-mail, fax, через Web-Систему регистрации запросов. Доступ к процедуре эскалации. Услуга предназначена для фиксирования обнаруженных неисправностей в созданной Исполнителем защищенной информационной системе передачи данных и слежения за их устранением.
2	Информирование Заказчика по телефону/email о факте регистрации запроса 1,2 приоритетов. 1 приоритет – обычная срочность; 2 приоритет – высокая срочность.	Дежурный инженер Исполнителя в течение времени регистрации запроса 1 и 2 приоритетов обязан связаться с клиентом для уточнения критичности сбоя и характера неисправности для скорейшей локализации и устранения проблемы. 1 приоритет – время регистрации составляет не более 30 минут; 2 приоритет – время регистрации составляет не более 15 минут.
3	Восстановление нормального функционирования оборудования и/или созданной защищенной информационной системы передачи данных	Удаленный поиск и устранение неисправности ПО и (или) Оборудования, приведение их функционирования к нормам, указанным в приемо-сдаточной документации. Работы специалиста Исполнителя по восстановлению работоспособности включают: <ul style="list-style-type: none">– диагностику оборудования и программного обеспечения;– анализ текущего характера взаимодействия компонентов поддерживаемого оборудования и программного обеспечения и их взаимодействия с другими

		компонентами информационной системы; – локализацию неисправности; – тестовую проверку работоспособности оборудования и программного обеспечения; – восстановление рабочего режима функционирования ПО и (или) Оборудования.
4	Информирование Заказчика о факте устранения неисправности и о причинах ее вызвавших	Информирование Заказчика по e-mail и Web-Систему регистрации запросов об устранении неисправности и о причинах её вызвавших

2.3.6. В процессе и по итогам проведения работ Заказчику должна быть предъявлена следующая документация:

а) Пояснительная записка к техническому проекту на создание защищенной информационной системы передачи данных, включающая в себя:

- 1) Структурную схему защищенной информационной системы передачи данных;
- 2) Схему коммутации технических средств защищенной информационной системы передачи данных;

3) Логическую схему информационных потоков защищенной информационной системы передачи данных;

4) Перечень комплексов технических средств с указанием:

- адреса и места установки оборудования, его типа, IP адреса (в табличном виде);
- таблицы коммутации оборудования (с указанием имени физического интерфейса);
- используемые в сети vlan с указанием адреса объекта, IP-подсети, vlan id и описания.

5) описание логики работы системы, с указанием:

- используемых в защищенной информационной системе передачи данных технологий и протоколов с привязкой к оборудованию;
- функционала сетевого оборудования и средств защиты;

б) Эксплуатационная документация на созданную защищенную информационную систему передачи данных:

1) Инструкцию администратора защищенной информационной системы передачи данных, включающей в себя подразделы с описанием работы для каждого компонента (подсистемы), в т.ч.:

- настройка интерфейсов, правил межсетевого экранирования, шифрования;
- настройка правил для подсистемы обнаружения и предотвращения вторжений;
- порядка смены паролей и сертификатов в случае компрометации и окончания их срока действия.

Инструкция должна быть подготовлена для созданной защищенной системы с использованием снимков экрана (скриншотов) отражающих эксплуатируемую Заказчиком защищенную информационную систему передачи данных;

2) Инструкцию по резервному копированию настроек для следующих подсистем:

- подсистемы обнаружения вторжений;
- подсистем межсетевого экранирования и криптографической защиты открытых каналов связи.

3) Руководство по установке оборудования;

4) Руководство по развертыванию (подключению) новых объектов (площадок);

5) таблица с учетными данными для административного доступа к оборудованию;

в) Рабочая документация на созданную защищенную информационную систему передачи данных, включающая в себя:

1) Программу и методику испытаний защищенной информационной системы передачи данных;

2) Программу опытной эксплуатации защищенной информационной системы передачи данных;

3) Проекты протоколов и формы актов для опытной эксплуатации и приёмо-сдаточных испытаний:

- Акт приёмки в опытную эксплуатацию защищенной информационной системы передачи данных;
- Протокол устранения замечаний;
- Протокол приёмочных испытаний;
- Акт приёмки в промышленную эксплуатацию защищенной информационной системы передачи данных.

3. Требования к Участникам:

3.1. Участник должен обладать практическим опытом выполнения работ по защите информационных систем, обрабатывающих персональные данные.

3.2. Исполнитель должен обладать лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации.

3.3. Исполнитель должен обладать лицензиями ФСБ России на деятельность по распространению и техническому обслуживанию шифровальных (криптографических) средств.

3.4. Исполнитель должен иметь в своем штате минимум 5 исполнителей, имеющих профильное высшее специальное образование в области информационной безопасности, либо прошедших обучение на курсах повышения квалификации по программам, согласованным с ФСТЭК России и ФСБ России, по соответствующим направлениям.

3.5. Участник должен предоставить авторизационные письма в адрес ОАО «Томскэнергосбыт» от производителей оборудования McAfee и S-Terra.

Примечание: соответствие всем вышеназванным требованиям должно быть письменно подтверждено соответствующими документами, в том числе по составу исполнителей и их образования в области защиты информации.

3.6. Участник не должен являться неплатежеспособным или банкротом, находиться в процессе ликвидации, на имущество участника в части, существенной для исполнения договора, не должен быть наложен арест, экономическая деятельность участника не должна быть приостановлена.

3.7. Наличие практического опыта выполнения аналогичных работ не менее 2 (двух) лет;

3.8. Отсутствие претензий со стороны заказчиков, к качеству выполненных работ и срокам исполнения договорных обязательств.

4. Требования к поставляемому оборудованию

4.1. Все поставляемое оборудование должно быть новыми. Оборудование по своим параметрам должно соответствовать требованиям, указанным в Приложении 1 к настоящему техническому заданию;

4.2. Условия хранения и транспортировки оборудования должно соответствовать требованиям производителя;

4.3. Оборудование и ПО должно поставляться с необходимыми для работы лицензиями;

4.4. Оборудование должно быть упаковано в заводскую упаковку;

4.5. Оборудование должно обеспечивать устойчивую работу в условиях колебаний напряжения и частоты переменного тока электрической сети в пределах, соответствующих стандартам на электроснабжение потребителей РФ;

4.6. В составе стандартной поставки оборудования должны присутствовать все драйверы и программное обеспечение, необходимое для эксплуатации оборудования;

4.7. Оборудование должно поставляться в комплекте со шнурами питания и иным вспомогательным оборудованием в соответствии с требованиями руководства по эксплуатации;

4.8. Оборудование должно поставляться в комплекте с гарантийным талоном;

4.9. Все поставляемые средства защиты должны быть сертифицированы федеральной службой по техническому и экспортному контролю, либо федеральной службой безопасности, что должно быть подтверждено соответствующими документами;

4.10. Не допускается поставка повторно восстановленной, имеющей механические повреждения продукции и её упаковки, выставочных образцов, а также продукции, условия хранения которой были нарушены;

4.11. Упаковка и маркировка оборудования должна содержать все признаки оригинальности, установленные производителями:

- производственный номер на коробке и товаре должны совпадать;
- корпус на поставляемом изделии не должен иметь потертостей, царапин, сколов и следов вскрытия;
- упаковка поставляемого оборудования должна быть новой, не поврежденной.

4.12. Заказчик вправе провести экспертизу поставленного оборудования в сервисном центре производителя или компании, авторизованной производителем, и, в случае получения заключения о не оригинальности продукции, вправе обратиться в компетентные органы, занимающиеся вопросами незаконного использования чужого товарного знака и участия в обороте контрафактной продукции. В случае получения заключения о не оригинальности продукции, весь поставленный товар не возвращается и оплата по нему не производится.

5. Условия оплаты и поставки:

5.1. В цену оборудования должна быть включена:

- стоимость оборудования, включая его принадлежности и расходные материалы;
- стоимость транспортировки до Заказчика, включая все сопутствующие расходы, такие как расходы по хранению, страхованию, оплате таможенных пошлин, НДС, налогов, сборов и других обязательных платежей;
- стоимость тары, упаковки, а так же приспособлений, необходимых для передачи оборудования.

5.2. Поставка оборудования должна быть произведена в течении 3-х недель;

5.3. Доставка осуществляется в рабочие дни, с 08:00 до 12:00 и с 12:00 до 16:30;

6. Требования к гарантийным обязательствам

6.1. Поставляемое оборудование, должно соответствовать заявленным техническим требованиям

6.2. Исполнитель гарантирует отсутствие в поставляемой продукции дефектов, возникающих из-за неправильного проектирования, применения дефектных материалов и/или некачественного выполнения работ на заводе-производителе.

6.2. На поставляемое оборудование должна предоставляется гарантия производителя, но в любом случае, не менее 12 месяцев от даты поставки.

6.3. На предоставляемые работы по созданию защищенной информационной системы передачи данных должна предоставляться гарантия не менее 12 месяцев с даты подписания акта выполненных работ.

7. График оказания работ

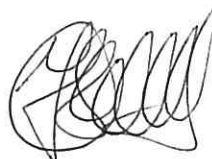
Начало выполнения работ: с момента подписания договора.

Окончание выполнения работ: в течение 120 дней с момента подписания договора.

8. Проект Договора Приложение №2

По всем вопросам, касающимся технического задания, обращаться к ведущему специалисту по информационной безопасности Соболеву Артёму Евгеньевичу, по тел: (3822) 48-49-00, sobolev@ensb.tomsk.ru.

Начальник отдела
экономической безопасности



В.Н. Соловьев

Технические требования к поставляемым средствам защиты

1. ПАК G-3000-L-5041-4-RED- KC2

Требования по функционалу:

Программно-аппаратный комплекс (ПАК) должен уметь выполнять следующие функции: межсетевое экранирование, построение виртуальных частных сетей (VPN), обеспечение стойкого шифрования передаваемой информации.

ПАК должен иметь возможность обеспечения защиты и фильтрации трафика сетей и служебного трафика.

ПАК должен поддерживать возможность удаленного управления через консоль (CLI) посредством протокола SSH, через Web-интерфейс и через систему централизованного управления.

Скорость шифрования должна быть не менее 350 Мбит/с на TCP трафике при использовании алгоритмов шифрования с проверкой целостности.

Количество одновременных защищенных соединений: до 1000 туннелей.

ПАК должен обеспечивать пакетную фильтрацию трафика с использованием информации в полях заголовков сетевого и транспортного уровней.

ПАК должен иметь возможность обеспечивать поддержку гибкой настройки правил обработки трафика на каждом интерфейсе.

ПАК должен уметь маскировать реальный IP адрес (туннелирование трафика).

ПАК должен поддерживать технологии протоколирования событий (syslog) и мониторинга глобальной статистики по протоколу SNMP.

ПАК должен поддерживать следующие алгоритмы:

шифрование ГОСТ 28147-89,

электронно-цифровая подпись ГОСТ Р 34.10-2001,

вычисление хэш сумм ГОСТ Р 34.11-94.

ПАК должен поддерживать работу через NAT.

ПАК должен поддерживать работу по протоколам IKE/IPsec согласно стандартам RFC 2401 – 2412.

ПАК должен иметь возможность получения сертификатов открытых ключей по протоколу LDAP, возможность импорта и доставки через PKCS#7, PKCS#12.

ПАК должен поддерживать использование списка отозванных сертификатов CRL.

Требования по физическим характеристикам:

Корпус 1U с возможностью установки в стойку 19".

Процессор с частотой не менее 3.1 Ghz.

Не менее 4Гб ОЗУ типа DDR3.

Не менее 4 сетевых интерфейсов GigabitEthernet.

Требования к надежности:

Гарантийный срок не менее 12 мес.

Температурный диапазон работы 10-35 °С

Относительная влажность окружающей среды 20-90%

Требования к сертификации:

ПАК должен иметь сертификат ФСБ России на соответствие требованиям к СКЗИ класса KC2 и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.

2. ПАК G-1000-L-5007-3-KC2

Требования по функционалу:

Программно-аппаратный комплекс (ПАК) должен уметь выполнять следующие функции: межсетевое экранирование, построение виртуальных частных сетей (VPN), обеспечение стойкого шифрования передаваемой информации.

ПАК должен иметь возможность обеспечения защиты и фильтрации трафика сетей и служебного трафика.

ПАК должен поддерживать возможность удаленного управления через консоль(CLI) посредством протокола SSH, через Web-интерфейс и через систему централизованного управления.

Скорость шифрования должна быть не менее 10 Мбит/с на TCP трафике при использовании алгоритмов шифрования с проверкой целостности.

Количество одновременных защищенных соединений: не менее 50 туннелей.

ПАК должен обеспечивать пакетную фильтрацию трафика с использованием информации в полях заголовков сетевого и транспортного уровней.

ПАК должен иметь возможность обеспечивать поддержку гибкой настройки правил обработки трафика на каждом интерфейсе.

ПАК должен уметь маскировать реальный IP адрес (туннелирование трафика).

ПАК должен поддерживать технологии протоколирования событий (syslog) и мониторинга глобальной статистики по протоколу SNMP.

ПАК должен поддерживать следующие алгоритмы:

шифрование ГОСТ 28147-89,

электронно-цифровая подпись ГОСТ Р 34.10-2001,

вычисление хэш сумм ГОСТ Р 34.11-94.

ПАК должен поддерживать работу через NAT.

ПАК должен поддерживать работу по протоколам IKE/IPsec согласно стандартам RFC 2401 – 2412.

ПАК должен иметь возможность получения сертификатов открытых ключей по протоколу LDAP, возможность импорта и доставки через PKCS#7, PKCS#12.

ПАК должен поддерживать использование списка отозванных сертификатов CRL.

Требования по физическим характеристикам:

Корпус 1U с возможностью установки в стойку 19".

Процессор с частотой не менее 1 Ghz.

Не менее 512Мб ОЗУ типа DDR2.

Энергонезависимая память не менее 1 Гб типа DOM.

Не менее 2 сетевых интерфейсов GigabitEthernet.

Требования к надежности:

Гарантийный срок не менее 12 мес.

Температурный диапазон работы 5-35 °С

Относительная влажность окружающей среды 20-80%

Требования к сертификации:

ПАК должен иметь сертификат ФСБ России на соответствие требованиям к СКЗИ класса КС2 и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.

3. ПК С-Х-WIN-KC2

Требования по функционалу:

Средство должно поставляться в виде программного комплекса (ПК);

ПК должен уметь выполнять следующие функции: межсетевое экранирование, построение виртуальных частных сетей (VPN), обеспечение стойкого шифрования передаваемой информации;

ПК должен иметь возможность обеспечения защиты и фильтрации трафика сетей и служебного трафика;

ПК должен обеспечивать пакетную фильтрацию трафика с использованием информации в полях заголовков сетевого и транспортного уровней;

ПК должен уметь маскировать реальный IP адрес (туннелирование трафика);

ПК должен поддерживать технологии протоколирования событий (syslog) и мониторинга глобальной статистики по протоколу SNMP;

ПК должен поддерживать установку в режиме One-Click-Installation (OCI) с использованием Windows Installer (MSI);

ПК должен поддерживать работу через NAT;
ПАК должен поддерживать работу по протоколам IKE/IPsec согласно стандартам RFC 2401 – 2412;
ПК должен поддерживать следующие алгоритмы:
шифрование ГОСТ 28147-89;
электронно-цифровая подпись ГОСТ Р 34.10-2001;
вычисление хэш сумм ГОСТ Р 34.11-94;
ПК должен иметь возможность получения сертификатов открытых ключей по протоколу LDAP, возможность импорта и доставки через PKCS#7, PKCS#12;
ПК должен поддерживать использование списка отозванных сертификатов CRL;
ПК должен быть совместим с ОС: MS Windows XP Professional (SP3), MS Windows Vista (SP2), MS Windows 7, Microsoft Windows Server 2003/2008;
ПК должен иметь сертификат ФСБ России на соответствие требованиям к СКЗИ класса КС2 и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.

4. Система централизованного управления КР-100

Требования по функционалу:
Программное обеспечение Система централизованного управления с числом поддерживаемых устройств не менее 100.
Программное обеспечение должно позволять контролировать активность устройств и сроки выдачи сертификатов управляемых устройств.
Программное обеспечение должно позволять изменять на управляемых устройствах:
Локальную политику безопасности.
Настройки политики драйвера.
Предопределенные ключи.
Сертификаты.
Списки отозванных сертификатов.
Настройки лога.
Лицензию VPN Агента.
Лицензию крипто-провайдера.
Клиента управления.
Программное обеспечение должно поддерживать следующие функции:
Сбор сообщений из журнала регистрации событий VPN-устройств.
Создание контейнеров с секретными ключами на VPN-устройстве.
Сбор настроек VPN-устройств непосредственно на VPN-устройствах.
Инициализация VPN-шлюзов со съемных носителей.
Конвертация политик безопасности VPN-устройств с младших версий на старшие.
Выполнение на VPN-устройстве расширенных сценариев обновления.
Программное обеспечение должно состоять из сервера управления и клиента управления, при этом сервер управления должен устанавливаться на выделенную рабочую станцию, клиент управления должен устанавливаться на выделенное VPN устройство.
Данные между клиентом и сервером должны передаваться по защищенному туннелю.
Обновления так же должны передаваться только по защищенным соединениям.
Инициатором сетевого взаимодействия должен быть клиент управления.
Программное обеспечение должно уметь централизованно обслуживать программные и аппаратные комплексы.
На сервере обязательно должен присутствовать консольный интерфейс управления данным программным продуктом.
Серверная часть должна работать под операционной системой Microsoft Windows 2003 или 2008, клиентская часть совместима с ОС других VPN-продуктов.

5. Система предотвращения вторжений StoneGate IPS-1205

Требования по функционалу:
Обнаружение и предотвращение попыток НСД в режиме реального времени в прозрачном для пользователей сети режиме;
Наличие сигнатур атак (по содержанию, контексту сетевых пакетов и другим параметрам);

Возможность борьбы с техниками обхода (evasions), включая их динамические варианты (AET);
Возможность контроля нескольких сетей с разными скоростями;
Декодирование протоколов для точного определения специфических атак, в том числе и внутри SSL соединений;
Возможность обновления базы данных сигнатур атак из различных источников (импорт сигнатур Open Source);
Возможность блокировки или завершения нежелательных сетевых соединений;
Анализ «историй» событий безопасности;
Анализ протоколов на соответствие RFC;
Встроенный анализатор событий;
Возможность создания собственных сигнатур атак, шаблонов анализа атак, аномалий;
Функциональность прозрачного межсетевого экрана Transparent Access Control;
Анализ GRE туннелей, сетей на базе протокола IPv6;
Централизованное управление и мониторинг;
Наличие сертификатов ФСТЭК России;
Поддержка функционала Web фильтрации, HA, VLAN инспекции.

Требования по производительности:

Количество одновременных поддерживаемых туннелей до 50;
Не менее шести интерфейсов 1000BASE-T;
Кол-во bypass интерфейсов – 4;
Общая производительность до 2 Гбит/сек;
Задержка на более 150 мсек;
Кол-во одновременных соединений – 1300000;
Соединений/сек – 50000;
SSL инспекция - 350Мбит/сек;
Кол-во сигнатур – 3500;

Требования по физическим характеристикам:

Не более 1U в высоту.

Система контроля трафика (IPS) должна позволять решать следующие задачи:

- должна предоставляться возможность ограничения доступа по произвольным протоколам стека TCP/IP на сетевом и транспортном уровне в соответствии с требованиями политики безопасности;
- динамическое определение работающих приложений и составление (в том числе) отчетов по ним, а также контроль использования приложений;
- возможность обнаружения работы несанкционированного ПО (spyware, программ удаленного управления, троянов и т.п.) и возможность его блокирования;
- управление и мониторинг из единой консоли администратора без необходимости доступа на локальную консоль;
- разбор и инспекция SSL/TLS трафика;
- возможность работы в «прозрачном» режиме по принципу L2-firewall;
- мониторинг трафика, циркулирующего на канальном, сетевом, транспортном и прикладном уровнях модели взаимодействия открытых систем с возможностью блокирования соответственно фреймов, пакетов, сегментов или датаграмм на каждом из уровней анализа;
- выявление и разбор технологий туннелирования трафика (например, GRE, IP-in-IP, IPv6-tunneling);
- создание собственных правил анализа;
- возможность URL фильтрации трафика по категориям, ведение белых и черных списков;
- работа в пассивном режиме как при копировании части трафика на устройство (span, tap, IDS), так и при установке в разрыв канала связи (inline, IPS), а также возможность комбинировать режимы работы в рамках одного исполнительного устройства;
- возможность пропуска части трафика без инспекции при перегрузке устройства в процессе инспекции трафика без вмешательства администратора (software bypass – функция должна быть настраиваемой, отключаемой);

- возможность корреляции группы или индивидуальных событий встроенными механизмами по порядку следования с целью создания сложных правил политики безопасности;
- оповещения администратора об обнаруженных атаках должно осуществляться как уведомлением на консоль, так и настраиваемыми сообщениями по электронной почте, уведомлениями SNMP-trap с индивидуальным конфигурированием под каждое из событий;
- вложенные и иерархические политики с правилами доступа, которые поддерживают «программируемые» элементы (т.е. элементы, которые могут принимать логические значения, а также изменять свое значение в зависимости от устройства, на которое они устанавливаются);

Требования к документации:

Программное обеспечение должно комплектоваться дистрибутивами с эксплуатационной документацией на CD или DVD.

Система анализа защищенности XSpider 7.8

Требования по функционалу:

Проверка на возможные уязвимости независимо от программной и аппаратной платформы узлов;

Работа с уязвимостями на разном уровне;

Анализатор защищенности WEB-серверов и WEB-приложений;

Идентификация сервисов на случайных портах;

Эвристический метод определения типов и имен серверов (HTTP, FTP, SMTP, POP3, DNS, SSH) вне зависимости от ответа на стандартные запросы;

Обработка RPC-сервисов (Windows и *nix) с их полной идентификацией;

Возможности определения RPC-сервисов и поиска уязвимостей в них, а также определения детальной конфигурации компьютера в целом;

Проверка слабости парольной защиты;

Подбор паролей в сервисах, требующих аутентификации;

Глубокий анализ контента WEB-сайтов;

Анализ скриптов HTTP-серверов и поиск в них разнообразных уязвимостей: SQL инъекций, инъекций кода, запуска произвольных программ, получения файлов, межсайтовый скриптинг (XSS), HTTP Response Splitting;

Анализатор структуры HTTP-серверов;

Поиск и анализ директорий доступных для просмотра и записи;

Проведение проверок на нестандартные DoS-атаки;

Возможность включения проверок "на отказ в обслуживании", основанных на опыте предыдущих атак и хакерских методах;

Графический интерфейс;

Планировщик заданий для автоматизации работы;

Одновременное сканирование большого числа компьютеров;

Ведение полной истории проверок;

Генерация отчетов с различными уровнями их детализации;

Встроенная документация;