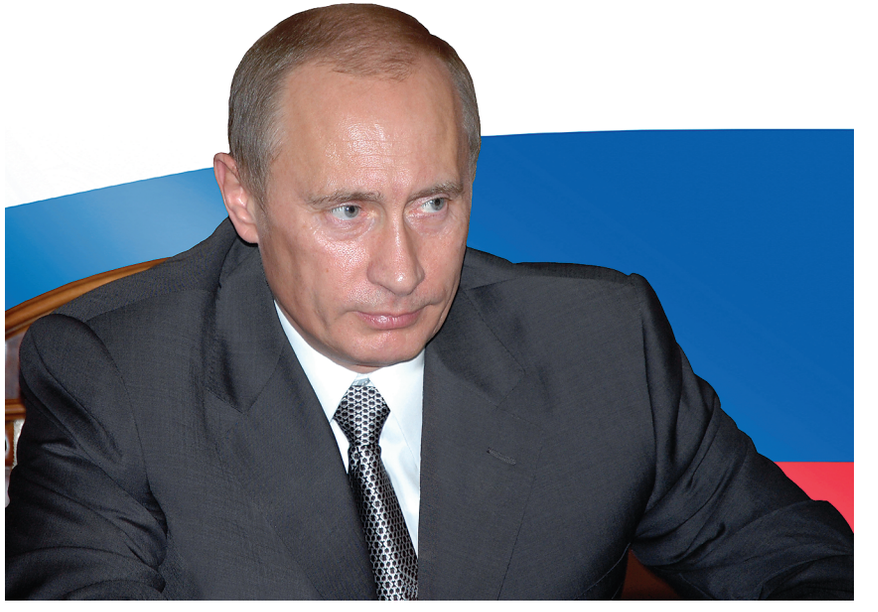
РОССИЙСКАЯ КОМПАНИЯ-РАЗРАБОТЧИК
КОМПЛЕКСНЫХ РЕШЕНИЙ IT-БЕЗОПАСНОСТИ «СМАРТ-СОФТ»

БЕЗОПАСНЫЙ ИНТЕРНЕТ В ГОСУДАРСТВЕННЫХ СТРУКТУРАХ. ИМПОРТОЗАМЕЩЕНИЕ 2.0



Россия должна по определению, вне зависимости от политической конъюнктуры, внедрять свои программные продукты и железо – это необходимо для собственного развития, и дело тут не в ограничениях и санкциях.

Президент РФ Владимир Путин
Источник: Экспертный центр электронного государства

Создание реестра отечественного ПО – не ответ на санкции, а последовательная политика мягкой поддержки собственных разработчиков.

Очень часто приходится видеть, когда заказчик, совершенно не думая, по старинке выбирает те или иные зарубежные продукты, хотя это несет и значительные затраты бюджетных средств, и риски информационной безопасности, и просто непонятно, почему настолько странное отношение было к отечественным разработчикам. Есть целый ряд серьезных конкурентоспособных продуктов.

Глава Минкомсвязи РФ Николай Никифоров
Источник: ИТАР-ТАСС

Опыт успешного применения отечественного ПО в муниципалитетах

С 1 января 2016 года действует постановление Правительства РФ, изменившее правила закупок программного обеспечения госсектором. Теперь для государственных и муниципальных нужд заказчики обязаны приобретать только российский софт, включенный в специальный реестр Минкомсвязи. Исключение – случаи, когда программно-аппаратные комплексы с необходимыми характеристиками в России отсутствуют. IT-специалисты российского госсектора уже активно изучают рынок отечественного программного обеспечения.

Эксперты компании «Смарт-Софт» обобщили опыт работы нескольких наиболее типичных представителей госсектора – администраций муниципалитетов, столкнувшихся с вопросом выбора отечественного межсетевого экрана в пользу Traffic Inspector. Этот программный продукт 18 марта включен в реестр российского программного обеспечения и имеет сертификацию ФСТЭК. Одни из представителей госсектора давно перешли на отечественные аналоги импортных средств защиты информации, другие сделали это сравнительно недавно.

Межсетевой экран, он же файервол – один из главных «защитников» корпоративной информации. Он защищает локальную сеть от несанкционированного доступа извне, от хакерских атак, попыток взлома или кражи информации и обеспечивает безопасный доступ пользователей к Интернету.

Администрация муниципального образования г. Губкинский (Ямало-Ненецкий автономный округ)

В администрации муниципального образования г. Губкинского до ноября 2015 года в качестве межсетевого экрана использовали иностранный аналог. На момент приобретения этого программно-аппаратного комплекса (в начале нулевых годов) выбирать было практически не из чего, поясняет Виктор Скусинец, главный специалист Управления информационных технологий и связи администрации города Губкинского. За 15 лет использования продукт морально устарел, его функционал не удовлетворял потребности IT-обеспечения деятельности администрации города. Программное обеспечение решено было сменить, и в ноябре 2015 года в Губкинском перешли на отечественный прокси-сервер.

– По каким критериям выбирали?

– Мы – бюджетная организация, и в соответствии с Федеральным законом № 44-ФЗ «О контрактной системе» провели аукцион на поставку средств защиты информации. Обязательным конкурсным требованием было наличие у программного комплекса сертификата ФСТЭК, подтверждающего, что использование данного софта безопасно. Traffic Inspector участвовал в конкур-

се и нашим требованиям удовлетворял. Продукт имеет необходимую сертификацию и конкурентоспособную цену, это полностью российский продукт. Его в результате аукциона и выбрали.

– Ожидаемые преимущества получили?

– Трудно судить о выгоде, поскольку приобретение файервола для нас было лишь одной из ступеней повышения уровня защиты информации. Нам нужно было изменить иерархию сети, и это удалось. Мы принципиально перестроили свою сеть, объединили в ней все бюджетные учреждения и организации нашего города. Вследствие этого потребовалось средство обеспечения безопасного доступа к Интернету. Предыдущий прокси-сервер лимитировал количество пользователей, а новый ограничений по числу пользователей не имеет. Так что напрямую сравнивать сложно, у нас получилась совершенно другая сеть.

– А недостатки?

– В новом софте не оказалось некоторых функций, к которым мы привыкли за 15 лет работы на старом, зарубежном продукте. Находимся в контакте с разработчиками и ждем от них обновлений. С прежним поставщиком такое было в принципе невозможно.

Администрация муниципального образования пос. Уренгой (Ямало-Ненецкий автономный округ)

Администрация муниципального образования поселок Уренгой отечественной комплексной системой информационной безопасности пользуется с 2008 года, рассказывает начальник отдела автоматизации и программного обеспечения администрации поселка Альбина Карпова.

– По каким критериям выбирали?
– Привлекательная для бюджетной организации цена и наличие качественной обратной связи с разработчиком. Приобретение иностранного программного обеспечения не рассматривали вообще – в частности, из-за невозможности получить высокий уровень техподдержки.

– Каков опыт использования Traffic Inspector?

– Качество защиты высокое. За время пользования этим программным комплексом не было ни одного факта несанкционированного доступа к сети организации. Адекватная техническая поддержка – это, как я уже сказала, для нас существенно. Traffic Inspector работает стабильно, к разработчикам мы обращались всего пару раз, при переходе со второй версии на третью, но важна уверенность в том, что техподдержка доступна и одни со своими

проблемами не останемся. Серьезное преимущество этого софта в том, что можно купить отдельные модули, непосредственно те, что нужны нам. Используем Traffic Inspector FSTEC в комплексе с NetPolice.

– Недостатки обнаружили?

– Не столько недостатки, сколько проблемные ситуации. У нас, например, не происходила синхронизация между публикацией служб и правилами внешнего сетевого экрана, при публикации службы с созданием правил во внешнем экране. Но это терпимо, на надежности защиты не сказывается, вопрос удобства эксплуатации. Продукт по нашим замечаниям дорабатывается и обновляется.

Администрация Емельяновского района (Красноярский край)

Опыт использования файервола Traffic Inspector администрацией Емельяновского района (Красноярский край) – более десяти лет. О нем рассказал Сергей Катков, системный администратор отдела по организационной работе и муниципальной службе администрации поселка.

— По каким критериям выбирали?

– Увидели, как работает это программное обеспечение в районном управлении образования, заинтересовались. Приобрели по доступной для бюджетной организации цене и успешно пользуемся. Импортные варианты средств защиты информации даже не рассматривали, неизвестно, что там зарубежные производители сделали и какие скрытые возможности доступа к нашей информации заложили в программу, и это не паранойя, инциденты такого рода документированы. К отечественному софту больше доверия, и он сертифицирован ФСБ, ФСТЭК.

– Каков опыт использования?

– Traffic Inspector позволяет избежать многих рисков. Защищает от вторжения на сервер, несанкционированного доступа. Даже если кто-то из сотрудников пытается подключиться к сети со своим ноутбуком, он не сможет этого сделать – Traffic Inspector ему не позволяет. Этот файервол отлично все закрывает. Вот пример: однажды наш провайдер доступа к Интернету решал свои технические задачи и для этого пытался отпинговать нас, но не смог этого сделать до тех пор, пока мы не отключили защиту.

Очень полезная дополнительная опция – возможность грамотно контролировать сетевую активность сотрудников и ограничивать при необходимости посещение непрофильных ресурсов (соцсети, торренты, новостные паблики и т. д.). Если нужно, ограничиваем время работы в сети, вводим иные ограничения.

В этом году приобрели новую версию программы. Стоимость более чем адекватна. Traffic Inspector на 200 пользователей без ограничений по времени использования обошелся нам в 67 тысяч рублей. У нас нет проблем ни с техподдержкой, ни с обновлениями. Головной боли с защитой информации тоже нет, мы довольны.

Резюмируя, перечислим доводы за использование в государственных организациях отечественного файервола:

1. Соблюдение российского законодательства.

2. Доступная цена, экономия бюджетных денег.

3. Адекватная и качественная техническая поддержка, доступная постоянно на родном языке.

4. Отсутствие закладок и бэкдоров гарантированно повышает информационную безопасность.

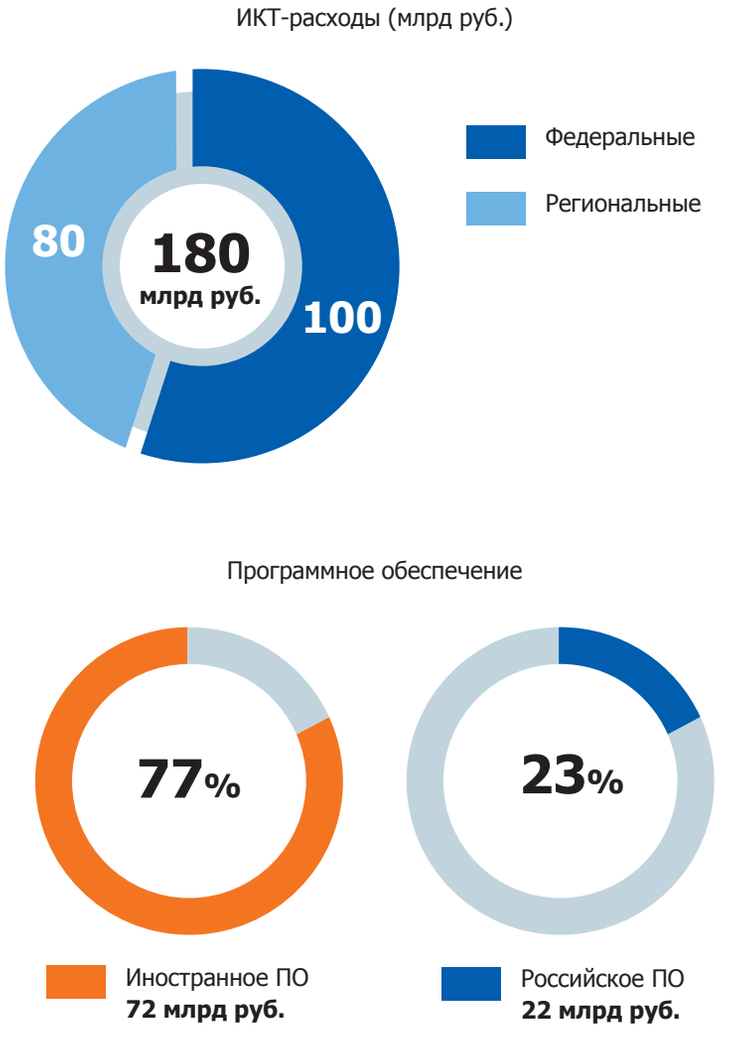
Еще один менее формальный, но не менее важный аргумент: при покупке за счет госбюджета российского программного продукта мы не просто возвращаем деньги налогоплательщиков в национальную экономику, а обеспечиваем этим деньгам многократный прирост. Особенность софтверной индустрии такова, что инвестиции в нее в конечном счете расходуются на образование, рост потребления, развитие высокотехнологичной индустрии. К этому имеет смысл стремиться.

ЦИФРЫ И ФАКТЫ

Органы государственной власти полностью зависимы от импортного программного обеспечения

По данным Минэкономразвития, 72,3% контрактов на закупку ПО органами государственной власти в 2015 году пришлись на зарубежные программные продукты, а в денежном выражении объем бюджетных средств, направленных на зарубежное программное обеспечение, составил 72 миллиарда рублей (77% всех расходов на эти цели).

ИКТ-закупки госорганов (по № 44-ФЗ), 2015 г.



По оценкам Экспертного центра электронного государства, ИКТ-закупки госорганов составили в 2015 году 180 миллиардов рублей, ИКТ-закупки госкомпаний – 310 миллиардов рублей, всего – 490 миллиардов рублей.

Источник: Экспертный центр электронного государства.

Интернет и законодательство

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 27.07.2006 Г. № 149-ФЗ «ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ»

ОСНОВНЫЕ МОМЕНТЫ:

СТАТЬЯ 15.1. ЕДИНЫЙ РЕЕСТР ДОМЕННЫХ ИМЕН, УКАЗАТЕЛЕЙ СТРАНИЦ САЙТОВ В СЕТИ ИНТЕРНЕТ И СЕТЕВЫХ АДРЕСОВ, ПОЗВОЛЯЮЩИХ ИДЕНТИФИЦИРОВАТЬ САЙТЫ В СЕТИ ИНТЕРНЕТ, СОДЕРЖАЩИЕ ИНФОРМАЦИЮ, РАСПРОСТРАНЕНИЕ КОТОРОЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ ЗАПРЕЩЕНО:

Часть 5

Основаниями для включения в реестр сведений являются:

1. Решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети Интернет:

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

д) информации, нарушающей требования Федерального закона от 29 декабря 2006 года N 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» и Федерального закона от 11 ноября 2003 года N 138-ФЗ «О лотереях» о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети Интернет и иных средств связи.

2. Вступившее в законную силу решение суда о признании информации, распространяемой посредством сети Интернет, информацией, распространение которой в Российской Федерации запрещено.

СТАТЬЯ 15.2. ПОРЯДОК ОГРАНИЧЕНИЯ ДОСТУПА
К ИНФОРМАЦИИ, РАСПРОСТРАНЯЕМОЙ С НАРУШЕНИЕМ
АВТОРСКИХ И (ИЛИ) СМЕЖНЫХ ПРАВ

Правообладатель в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети Интернет, объектов авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемых в таких сетях, или информации, необходимой для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без его разрешения или иного законного основания, вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с заявлением о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такие объекты или информацию, на основании вступившего в силу судебного акта.

СТАТЬЯ 15.3
В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети Интернет, информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, включая случай поступления уведомления о распространении такой информации от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан, Генеральный прокурор Российской Федерации или его заместители направляют требование в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

СТАТЬЯ 17, ЧАСТЬ 1
Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

ЧТО ЭТО ЗНАЧИТ ДЛЯ НАС С ВАМИ?

Что размещение всей указанной информации карается по закону (где-то Уголовным кодексом РФ, где-то Кодексом об административных правонарушениях, ну а где-то блокировкой сайта…).

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 27.07.2006 Г. № 152-ФЗ
«О ПЕРСОНАЛЬНЫХ ДАННЫХ»

ОСНОВНЫЕ МОМЕНТЫ:

СТАТЬЯ 3, ПУНКТЫ 1 И 3
Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных); обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

СТАТЬЯ 6, ЧАСТЬ 1, ПУНКТ 1
Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

СТАТЬЯ 7
Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

ЧТО ЭТО ЗНАЧИТ ДЛЯ НАС С ВАМИ?

Все Ваши персональные данные (фамилия, имя, отчество, адрес проживания и т. д.) могут собираться и распространяться только с Вашего разрешения. Если вдруг Вы обнаружите в сети Интернет информацию о себе, содержащую Ваши персональные данные, разрешение на размещение которых Вы не давали, требуйте от владельца сайта ее удаления. А в случае если Вам отказывают в удалении, обращайтесь в Роскомнадзор (см. ссылку ниже), в полномочия которого входят такие вопросы.

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 16 НОЯБРЯ 2015 Г. № 1236

«ОБ УСТАНОВЛЕНИИ ЗАПРЕТА НА ДОПУСК ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ПРОИСХОДЯЩЕГО ИЗ ИНОСТРАННЫХ ГОСУДАРСТВ, ДЛЯ ЦЕЛЕЙ ОСУЩЕСТВЛЕНИЯ ЗАКУПОК ДЛЯ ОБЕСПЕЧЕНИЯ ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ НУЖД»

ОСНОВНЫЕ МОМЕНТЫ:

В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» и Федеральным законом «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»

Правительство Российской Федерации постановляет:

1. Утвердить прилагаемые:

Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных (далее – реестр);
Порядок подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд.

2. Установить запрет на допуск программ для электронных вычислительных машин и баз данных, реализуемых независимо от вида договора на материальном носителе и (или) в электронном виде по каналам связи, происходящих из иностранных государств, а также исключительных прав на такое программное обеспечение и прав использования такого программного обеспечения (далее – программное обеспечение и (или) права на него), для целей осуществления закупок для обеспечения государственных и муниципальных нужд, за исключением следующих случаев:

а) в реестре отсутствуют сведения о программном обеспечении, соответствующем тому же классу программного обеспечения, что и программное обеспечение, планируемое к закупке;

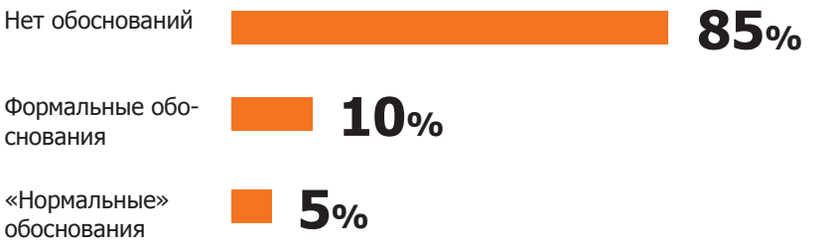
б) программное обеспечение, сведения о котором включены в реестр и которое соответствует тому же классу программного обеспечения, что и программное обеспечение, планируемое к закупке, по своим функциональным, техническим и (или) эксплуатационным характеристикам не соответствует установленным заказчиком требованиям к планируемому к закупке программному обеспечению.

ЧТО ЭТО ЗНАЧИТ ДЛЯ НАС С ВАМИ?

Установлен запрет на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд. В Едином реестре российских программ для электронных вычислительных машин и баз данных можно найти сведения об отечественном программном обеспечении. Если ПО в реестре не соответствует установленным заказчиком требованиям к планируемому к закупке программному обеспечению, то запрет не действует.

По результатам I квартала 2016 года можно констатировать, что Постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» практически не выполняется.

Закупки иностранного ПО, I квартал 2016 г.



Органы власти по-прежнему активно закупают иностранное ПО и, более того, даже не удосуживаются размещать обоснования о невозможности соблюдения запрета на такие закупки.

Так, по примерной оценке, 85% закупок органов власти СОВЕРШАЮТСЯ БЕЗ обоснований, около 10% имеют формальные обоснования и только 5% - с документами в соответствии с требованиями постановления.

В настоящее время, по данным Минкомсвязи, объем ежегодных лицензионных отчислений зарубежным производителям ПО составляет порядка 285 миллиардов рублей (45% от общего объема российского ПО), при этом 30% таких отчислений приходится на госсектор. По мнению министерства, зависимость РФ от зарубежных разработчиков программного обеспечения в течение 5–7 лет снизится на 30–50%.

«По нашим данным, только органы госвласти осуществляют закупку иностранного ПО примерно на 20 миллиардов рублей в год. При этом качественное решение у наших разработчиков есть, – заявил министр на встрече президента РФ Владимира Путина с членами правительства. – Теперь вместе с ФАС России будем ловить за руку тех госзаказчиков, кто все равно по старинке предпочитает закупать иностранное ПО, несмотря на то, что появились российские решения».

Источник: ТАСС.

Безопасная организация интернет-доступа в госструктуре

ОСНОВНЫЕ ЗАДАЧИ

- Комплексная и качественная информационная безопасность.
- Соблюдение законодательства РФ: № 149-ФЗ, № 152-ФЗ, включая требования ФСТЭК.
- Защита персональных данных.
- Снижение стоимости продукта государственным структурам.

РЕШЕНИЕ

Traffic Inspector FSTEC идеально подходит организациям государственного сектора в рамках государственной программы импортозамещения и повышения эффективности технических средств информационной безопасности.

Продукт выпускается российской компанией ООО «Смарт-Софт», которая обладает 13-летним опытом разработки и реализации корпоративных систем защиты информации и управления интернет-доступом. Компания имеет собственные разработки на основе уникальных запатентованных программных алгоритмов, полностью соответствующих требованиям Российского законодательства в области защиты информации, а также все необходимые лицензии и сертификаты.

Проверен и рекомендован государственными структурами

Продукт полностью удовлетворяет критериям отечественного программного обеспечения, разработанным Министерством связи и массовых коммуникаций Российской Федерации. Traffic Inspector рекомендуют более 25 000 государственных организаций, которые его успешно используют: Федеральная налоговая инспекция, Министерство финансов Красноярского края, Министерство развития информационного общества Калужской области, администрация города Магнитогорска, ФБУ «Отдел финансового обеспечения Министерства обороны Российской Федерации по Челябинской, Тюменской и Курганской областям», аппарат правительства Республики Тыва, ФГУП «Почта России».

Сертифицирован и имеет необходимые лицензии и патенты

Компания «Смарт-Софт» лицензирована Федеральной службой по техническому и экспортному контролю (ФСТЭК) на деятельность по разработке и производству средств защиты конфиденциальной информации. Решение Traffic Inspector сертифицировано ФСТЭК РФ как средство защиты информации класса 1 ИСПДн, что подтверждает легитимность программы и позволяет выполнить требования российского законодательства. Имеются свидетельства Роспатента.

Создает доверенную среду

Неблагоприятные внешние факторы несут с собой значительные риски (IT-системы госсектора могут отключиться моментально/внепланово перестать функционировать/через некоторое время перестанут функционировать после введения санкций).

Это может произойти из-за отключения лицензионных ключей на стороне вендора, истечения срока действия лицензионных ключей, выхода из строя привязанного оборудования или удаленной активации «закладок». Traffic Inspector полностью убирает эти риски.

Стабилен по стоимости

Цена за лицензию программного обеспечения не привязана к курсу валют. Кроме того, при договоренности можно закрепить стоимость для ожидания поступления бюджетных денег.

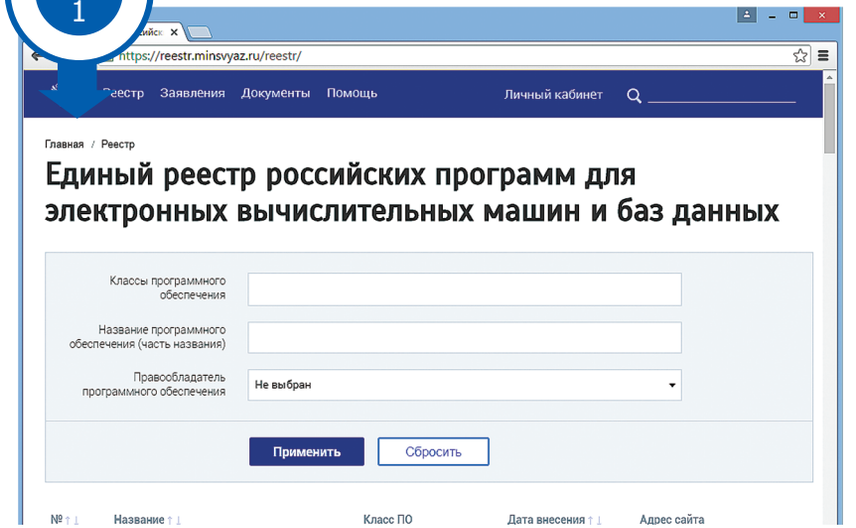
Характеристики Traffic Inspector

Функционал	Описание
Пользовательский интерфейс	Оснастка Microsoft Management Console
Версия протокола IP	IPv4
Поддержка сетевых технологий	IEEE 802.3 (Ethernet), 802.11 (Wi-Fi), PPP, VPN (PPTP, L2TP), IEEE 802.1Q (VLAN с использованием теггированного трафика
Преобразование сетевых адресов (NAT)	RRAS NAT (Windows), ICS NAT (Windows)
Производительность сетевого драйвера	600 Мбит/с при передаче IMIX-трафика
Типы пользователей	Пользователь, группа пользователей
Количество поддерживаемых пользователей	До 300 пользователей при работе через веб-прокси, до 1000 пользователей при работе в режиме NAT-шлюза
Аутентификация пользователей	BASIC / NTLM аутентификация, аутентификация по IP/MAC/VLAN ID, аутентификация через Клиентского агента
Файервол	Контекстный файервол, настраивается с помощью правил
Прокси-серверы	HTTP-прокси, SOCKS-прокси
HTTP-прокси	HTTP/1.1, FTP over HTTP, форвардинг SSL-соединений (метод HTTP CONNECT), прозрачный прокси, настраиваемые режимы кэширования, контентная фильтрация, фильтрация по URL, поддержка протокола Proxy Auto-Config
SMTP-сервер	Обеспечивает учет и фильтрацию входящего SMTP-трафика
Возможности расширенной маршрутизации	Резервирование каналов, маршрутизация по условию (решение о маршрутизации может приниматься на основе информации о сетевом протоколе, выходном интерфейсе, расписании, и т. д.), ограничение скорости работы пользователей и гурпп, приоритезация трафика
Интеграция с Microsoft Active Directory	Поддерживается импортирование пользователей из домена Active Directory
Поддержка баз данных	Microsoft SQL Server, MySQL, PostgreSQL, SQLite
Встроенный веб-сервер	Реализован как ASP.NET приложение; HTTP/1.1, поддержка keep-alive соединений, поддержка докачки файла, cache tagging; Поддерживаемые версии протокола SSL: TLS (SSL 3.1), SSL 3.0, SSL 2.0. SSL 1.0.
Защищенная передача данных	Основанное на использовании SSL-сертификата, защищенное соединение между Клиентским агентом и шлюзом Traffic Inspector, между веб-браузером и веб-порталом Traffic Inspector
Учет трафика и отчеты	Учет трафика реализован в виде счетчиков трафика и отчетов (отчет по пользователям, отчет по времени, отчет по скорости, сетевая статистика, отчет по активности пользователей, отчет антивируса, отчет веб-прокси), журнал действий администратора, оповещение по электронной почте
Системные требования	
Процессор	Процессор семейства Intel® Core™ 2
Оперативная память	2048 МБ
Операционная система	Microsoft Windows XP/2003/Vista/2008/7/2008 R2 или старше (версия x86 или x64)
Жесткий диск	1000 МБ + дополнительное пространство для хранения кэша прокси и файлов базы данных
Рекомендуемое разрешение	1024x768

Как найти межсетевой экран Traffic Inspector FSTEC в Едином реестре российских программ для электронных вычислительных машин и баз данных.

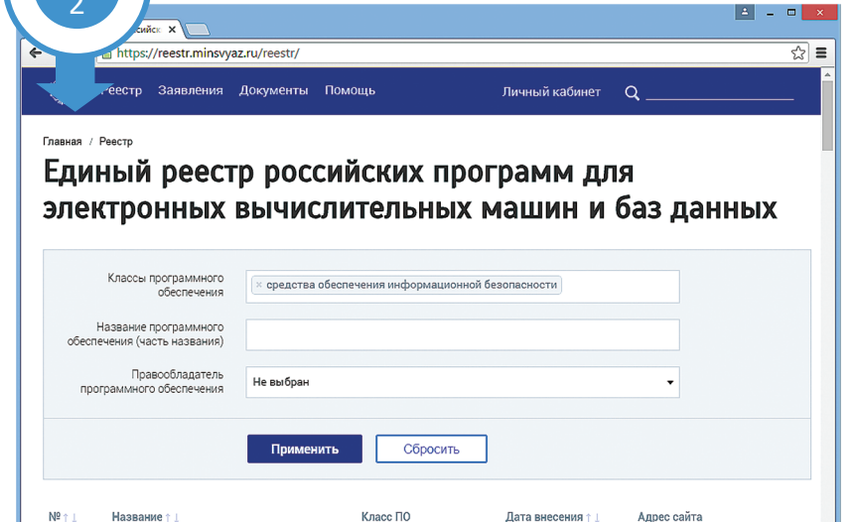
ШАГ 1

Зайти на сайт Единого реестра https://reestr.minsvyaz.ru/reestr/.



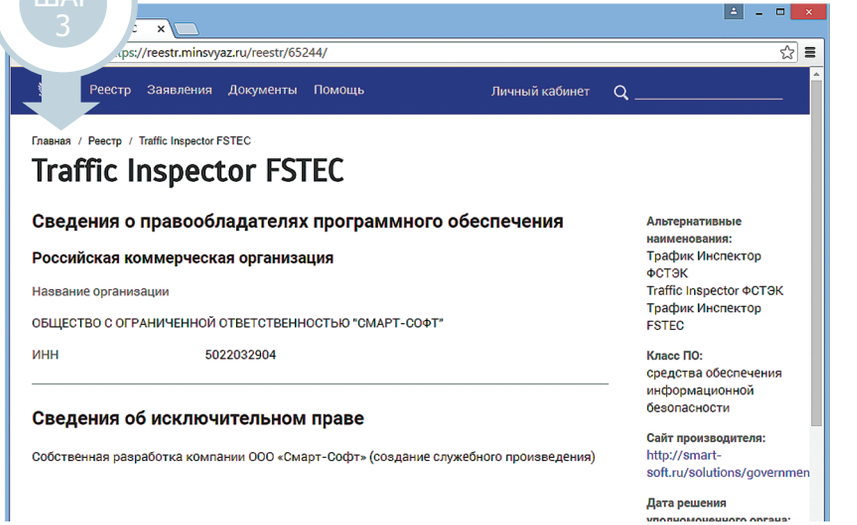
ШАГ 2

Выбрать вкладку «Класс программного обеспечения: средства обеспечения информационной безопасности».



ШАГ 3

Выбрать Traffic Inspector FSTEC.



ШАГ 4

Зайти на сайт производителя и узнать подробнее о продукте: www.smart-soft.ru.

Отзывы о работе Traffic Inspector в государственных структурах

– Хотелось бы поблагодарить менеджеров компании «Смарт-Софт», которые с вниманием и пониманием отнеслись к нашему запросу. Наша команда – сотрудники IT-департамента и руководство службы надеются на дальнейшее сотрудничество. Нам необходимы качественные российские программные продукты. Хотелось бы, чтобы в России было побольше таких стремительно развивающихся, крепко стоящих на ногах проектов.

Гюльванесян Эдуард,
заместитель начальника отдела информационных технологий УФНС России по КБР

– Уже 5 лет мы используем Traffic Inspector в своей школе и хотели бы отметить несомненные достоинства применения программы: экономия интернет-трафика, блокировка нежелательных сайтов и рекламы, простота и удобство пользования. Все это значительно улучшает образовательный процесс. Хотелось бы отметить гибкую ценовую политику вашей компании, которая предлагает особые условия для государственных учреждений.

Юрий Яббаров,
директор КГАОУ «Школа космонавтики»

– Работой программы довольны, трудностей при использовании не возникало – все ясно из справки к программе, сейчас планируем увеличить количество пользователей еще на 10 учетных записей. «Смарт-Софт», успехов, побольше программ, которые бы нам помогали в нашей работе.

Администрация музея-заповедника «Бородинское поле»

– Для организации работы с ресурсами глобальной сети ЦУКС МЧС России по Волгоградской области с 2006 года использует программное обеспечение Traffic Inspector, которое является единственным программным решением с очень гибкой структурой управления. Спасибо компании «Смарт-Софт». Мы вам доверяем!

Александр Югрин,
заместитель начальника ЦУКС МЧС России по Волгоградской области

История успешного внедрения программы Traffic Inspector FSTEC

Traffic Inspector FSTEC в Управлении ФНС России по Кабардино-Балкарской Республике

В работе УФНС России по КБР сделана ставка на использование информационных технологий и развитие онлайн-сервисов, электронного документооборота. При построении модулей информационной системы специалисты четко следуют корпоративным стандартам как в аппаратном, так и в программном обеспечении. Для функционирования достаточно сложной системы необходимо решать спектр задач, требующих дополнительного профессионального подхода.

Для эффективной работы сотрудников нашей службы необходим правильный подход к решению такой задачи, как оптимизация расхода трафика и безопасная работа в Сети. По итогам анализа рынка существующих проектов мы выбрали Traffic Inspector. Ведь проект является исключительно российской разработкой, позиционирует себя как комплексное сертифицированное сетевое решение для организации и контроля доступа в Интернет и обладает полным набором необходимого для нашего учреждения функционала. Можно заметить, что программный продукт динамично развивается и имеет множество положительных отзывов.

В штате УФНС России по КБР насчитывается более 100 рабочих мест. Комплексное решение Traffic Inspector идеально подходит под требования учреждения и реализовывает главную задачу – ограничение потребительского трафика от общего служебного. После решения поставленной задачи стало доступно подключение максимального количества рабочих мест к Сети с наиболее эффективным распределением, прекратилась бесконтрольная утечка трафика.

Установив Traffic Inspector, специалисты увидели гибкую, легко контролируемую систему интернет-доступа. Работа с программным продуктом стала частью ежедневной деятельности сотрудников налоговой службы. Удобный интерфейс помогает молодым администраторам легко справляться с управлением системой. Доступная система отчетов позволяет анализировать весь расход трафика. Полный функционал продукта направлен на эффективную работу системного администратора и, следовательно, службы в целом.

Нами была успешно внедрена версия Traffic Inspector, сертифицированная ФСТЭК. Сейчас наши специалисты решили расширить применение продукта и работают над тем, чтобы наиболее эффективно встроить его в узкие рамки корпоративных стандартов. Версия продукта ФСТЭК позволяет реализовывать весь функционал программного решения Traffic Inspector.

О КОМПАНИИ

Партнеры

2 500 ПАРТНЕРОВ

Более 2 500 партнеров на российском и международном рынках

Пользователи

4 500 000 ЧЕЛОВЕК

4 500 000 человек работают в сетях, где установлены наши решения

Уверенность в завтрашнем дне

13 ЛЕТ

13 лет на рынке информационной безопасности

КОНТАКТЫ

Звоните: +7 (495) 77-55-991
Пишите: info@smart-soft.ru
www.smart-soft.ru

© 2003-2016, ООО «Смарт-Софт», www.smart-soft.ru