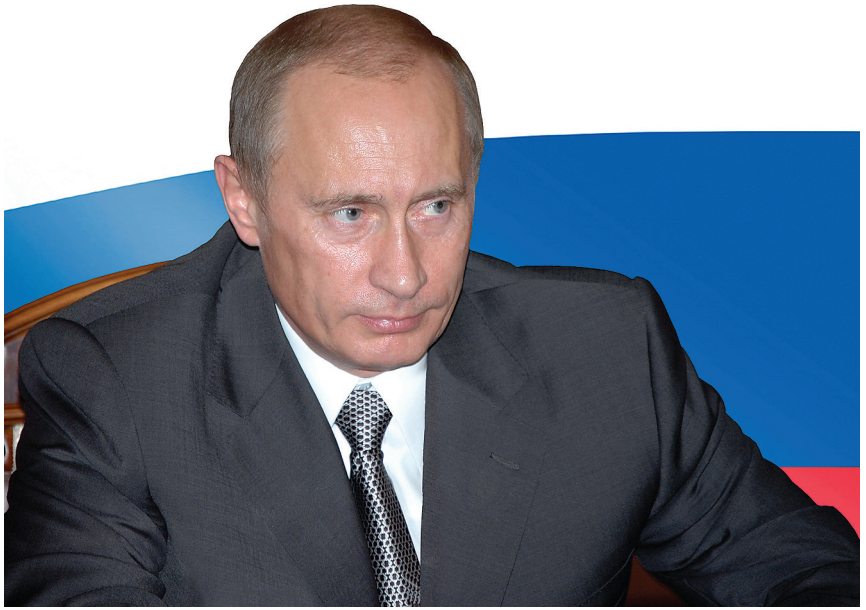
РОССИЙСКАЯ КОМПАНИЯ-РАЗРАБОТЧИК
КОМПЛЕКСНЫХ РЕШЕНИЙ IT-БЕЗОПАСНОСТИ «СМАРТ-СОФТ»

Безопасный Интернет в государственных структурах. Импортозамещение-2018

2018 г.



Мы должны четко представлять тенденции развития глобальной информационной сферы, прогнозировать потенциальные угрозы и риски и, главное, наметить дополнительные меры, которые позволят нам не просто своевременно выявлять угрозы, а активно реагировать на них.

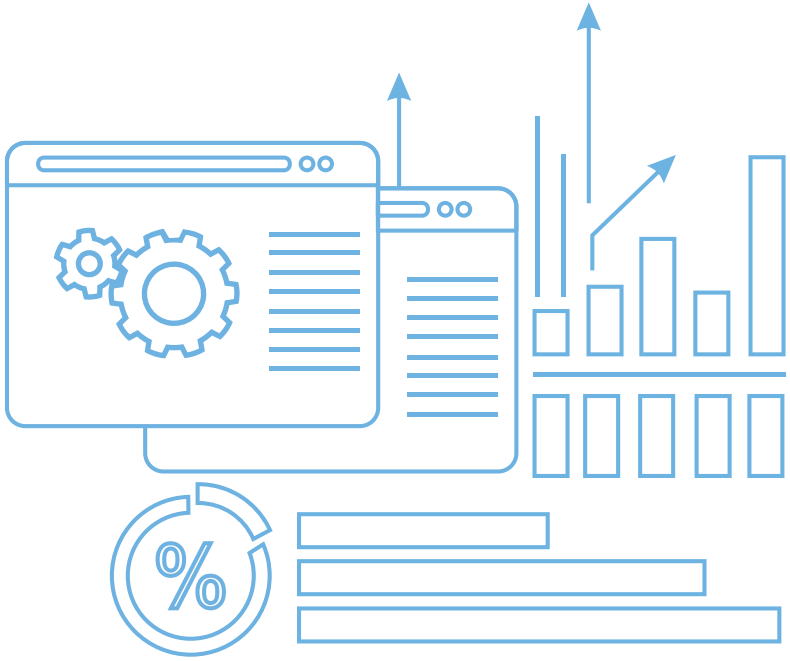
Первое – это совершенствование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России. Второе – это повышение защищенности информационных систем и систем связи государственных органов. Считаю, что нужно усилить персональную ответственность руководителей для обеспечения информационной безопасности.

Президент РФ Владимир Путин
Источник: ИНТЕРФАКС

Я считаю, что РФ и многим другим странам необходимо продолжить выделять ресурсы, время, усилия на то, чтобы диверсифицировать мировую IT-экосистему. Мы очень зависим от определенных компаний-монополистов, эти компании всем хорошо известны. Мы считаем, что в этом есть определенный риск, определенная угроза с точки зрения в том числе информационной безопасности.

Глава Минкомсвязи РФ Николай Никифоров
Источник: РИА Новости

Общая ситуация на рынке



Текущая ситуация на российском рынке программного обеспечения обусловлена совокупностью следующих факторов:

1. Ограничение возможности закупки иностранного программного обеспечения (ПО) для некоторых секторов российской экономики в результате антироссийских санкций.

2. Скачкообразный рост стоимости зарубежного ПО в результате резкого падения курса рубля к иностранным валютам.

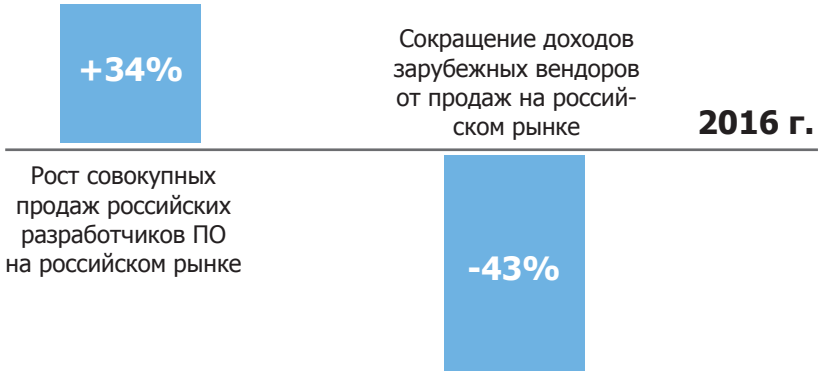
3. Принятие ряда законов и подзаконных актов, направленных на ограничение закупок иностранного ПО для государственных и муниципальных организаций, а также для компаний с государственным участием.

4. Принятие пакета законов, регулирующих работу с персональными данными, критической информационной инфраструктурой РФ и блокировку сайтов с запрещённой информацией.

5. Разработка государственных мер поддержки отечественных разработчиков ПО: создание единого реестра российских программ и Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий.

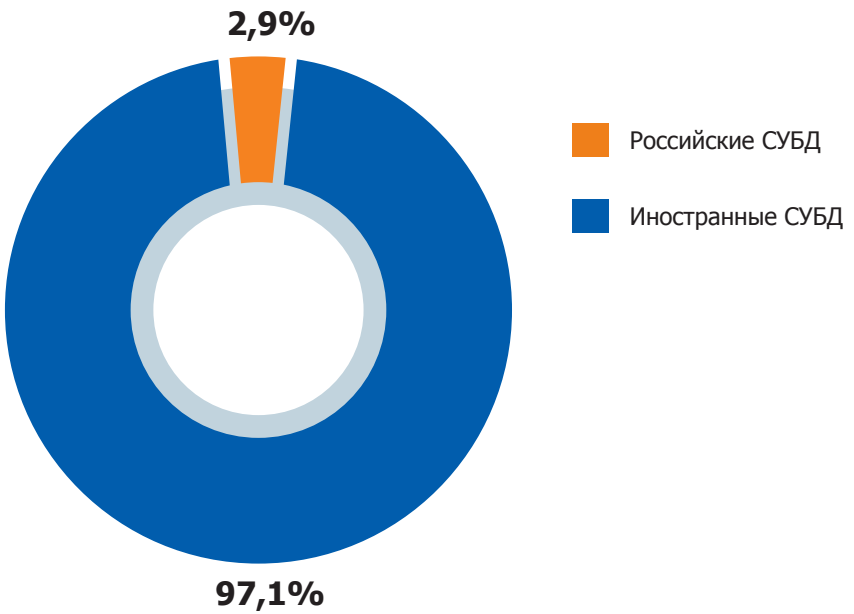
Стоимость ПО российской разработки может отличаться от аналогичных по функциональности зарубежных в десятки раз. Кроме того, рублёвые цены на иностранные продукты менялись с задержкой по отношению к изменению курса рубля. В связи с этим напрямую оценить изменения, происходящие на рынке ПО, крайне сложно. Тем не менее, согласно исследованиям, проведённым компаниями «Руссофт» и «Код безопасности»:

• В 2016 г. российские разработчики ПО увеличили совокупные продажи на внутреннем рынке на 34%, а доходы зарубежных вендоров сократились на 43%. Однако импортозамещение происходило в первую очередь в тех сегментах, в которых зарубежные вендоры не доминировали.



• По данным на начало осени 2017 г., импортозамещение почти не коснулось федеральных государственных информационных систем (ФГИС): доля систем управления базами данных (СУБД) MS SQL Server и Oracle в 2017 году составляла 38,6% и 25,4%, в 2015 – 41,1% и 28%. Российские СУБД используются лишь в 2,9% ФГИС.

Доли иностранных и российских СУБД, используемых ФГИС



• Во втором квартале 2017 г. госкомпании потратили на покупку продуктов Microsoft 668 млн рублей – в шесть раз меньше, чем во втором квартале 2016 г.

Расходы госкомпаний на покупку продуктов Microsoft, млн руб.

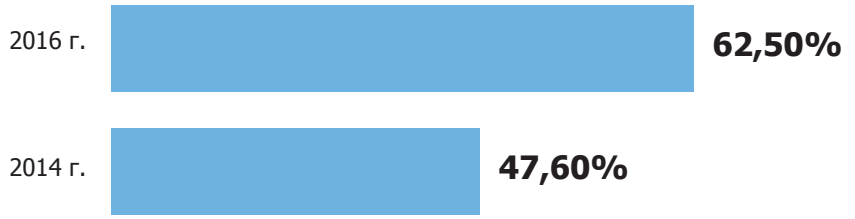
• Госорганы за I полугодие 2017 г. потратили на продукты Microsoft на 4 млн рублей меньше, чем за аналогичный период 2016 г., и на 91 млн рублей меньше, чем в первой половине 2015 г.

Затраты госорганов на продукты Microsoft, млн руб.

• В портфеле применяемых решений по информационной безопасности всех отраслей, кроме топливно-энергетического комплекса, доля российских решений составляла в 2016 г. более 50%. Эта величина продолжила рост в 2017 году.

• Увеличилось количество государственных организаций, где доля российских решений по информационной безопасности составляет более 75%. Если в 2014 г. структур с таким уровнем потребления отечественных средств защиты информации было 47,6%, то к концу 2016 г. – уже 62,5%.

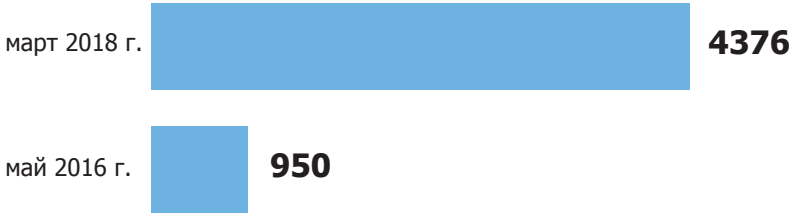
Процент государственных организаций, где доля российских ИБ-решений составляет более 75%



Постановление № 1236 об ограничении закупок иностранного ПО для государственных и муниципальных нужд вступило в действие 1 января 2016 года. Чтобы помочь государственным и муниципальным организациям реализовать требования постановления по использованию преимущественно отечественного ПО, в 2016 году был создан Центр компетенций по импортозамещению в сфере информационно-коммуникационных технологий.

Созданный в рамках политики импортозамещения реестр отечественного ПО постоянно пополняется новыми разработками: по состоянию на 20.05.2016 года реестр содержал 950 программ, а уже в конце марта 2018 года – более 4300.

Количество отечественных программ, включенных в Единый реестр российских программ для электронных вычислительных машин и баз данных, шт.



Благодаря ограничительным мерам и созданию реестра у небольших разработчиков появилась возможность предложить свои разработки госзаказчикам и получить преимущества перед иностранными вендорами с практически неограниченными бюджетами.

Несмотря на запрет, государственные и муниципальные организации продолжают размещать заявки на приобретение иностранного ПО, не пытаясь подобрать альтернативные решения из реестра. Если раньше можно было списать такой подход на незнание или отсутствие в реестре программ с необходимыми функциями, то сейчас для наиболее востребованных решений имеется вполне достойная альтернатива.

За время работы Центра компетенций по импортозамещению были аннулированы несколько закупок ПО, в частности закупки Росархивом и Министерством иностранных дел РФ программ Microsoft.

Интернет и законодательство

В РФ принят ряд законов, регулирующих доступ к сайтам с запрещённой информацией, работу с персональными данными и приобретение программного обеспечения. Все государственные и муниципальные организации обязаны принять меры по соблюдению требований этих законов.

РЕЕСТР САЙТОВ С ЗАПРЕЩЁННОЙ ИНФОРМАЦИЕЙ

Закон № 149-ФЗ «Об информации, информационных технологиях и защите информации» вводит понятие реестра сайтов, содержащих запрещённую в РФ информацию:

- детскую порнографию, сведения о наркотиках, самоубийствах, азартных играх и несчастных случаях с несовершеннолетними;
- фильмы, книги, фотографии, музыку и другую информацию, защищённую авторскими правами;
- призывы к насилию, экстремизму и массовым беспорядкам.

ГЛАВНОЕ

Согласно требованиям закона, доступ к сайтам, включённым в реестр, должен быть ограничен. За нарушение этих требований предусмотрена дисциплинарная, гражданско-правовая, административная и уголовная ответственность. Чтобы избежать наказания, организации обязаны соблюдать требования законодательства и блокировать доступ пользователей к сайтам из реестра.

Реализовать блокировку в соответствии с законодательством РФ помогут многофункциональный межсетевой экран и система обнаружения (предотвращения) вторжений Traffic Inspector и универсальный шлюз безопасности (UTM) и система обнаружения (предотвращения) вторжений Traffic Inspector Next Generation, входящие в Единый реестр российских программ.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Закон № 152-ФЗ «О персональных данных» определяет порядок работы с информацией, прямо или косвенно относящейся к физическому лицу. В частности, статья 19 закона определяет обязанности оператора по обеспечению безопасности персональных данных при их обработке:

- применение организационных и технических мер;
- применение средств защиты информации, прошедших процедуру оценки соответствия;
- обнаружение фактов несанкционированного доступа к персональным данным;
- установление правил доступа к персональным данным.

На основании части 4 статьи 19 Закона № 152-ФЗ ФСТЭК издала приказ № 21 от 18.02.2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». В соответствии с приказом в состав мер по обеспечению безопасности персональных данных также входят:

- регистрация событий безопасности;
- обнаружение и предотвращение вторжений;
- защита информационной системы, её средств, систем связи и передачи данных.

ГЛАВНОЕ

Если государственное или муниципальное учреждение производит работу с персональными данными, оно обязано использовать средства защиты информации для защиты своих информационных систем, причем средство защиты информации должно пройти процедуру оценки соответствия, обнаруживать и предотвращать вторжения, регистрировать события безопасности и защищать информационную систему, устанавливая правила доступа к персональным данным.

Обеспечить защиту информационных систем в соответствии с законодательством РФ помогут сертифицированный многофункциональный межсетевой экран Traffic Inspector FSTEC и сертифицированный универсальный шлюз безопасности (UTM) Traffic Inspector Next Generation FSTEC, прошедшие сертификацию на соответствие требованиям ФСТЭК России к межсетевым экранам, утвержденным в Информационном сообщении ФСТЭК № 240/24/1986 от 28 апреля 2016 года.

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА РФ

С 1 января 2018 года вступил в действие Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Согласно закону, критическая информационная инфраструктура (КИИ) представляет собой совокупность объектов КИИ - информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления субъектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия таких объектов.

Субъектами КИИ являются государственные органы и учреждения, российские юридические лица и/или индивидуальные предприниматели, которым принадлежат объекты КИИ, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах фи-

нансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и/или индивидуальные предприниматели, которые обеспечивают взаимодействие объектов КИИ.

Федеральный закон № 187-ФЗ предусматривает уголовную ответственность за кибератаки на инфраструктуру организаций, отнесённых к субъектам КИИ.

Статья 9 закона накладывает на организации и компании, относящиеся к субъектам КИИ, ряд обязанностей, в числе которых:

- соблюдение требований по обеспечению безопасности (статья 11 закона);
- незамедлительная реакция на компьютерные инциденты;
- оповещение уполномоченных организаций.

Согласно Приказу ФСТЭК № 235 от 21 декабря 2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ, относятся средства защиты информации, в том числе средства защиты информации от несанкционированного доступа, межсетевые экраны, средства обнаружения и предотвращения вторжений, средства антивирусной защиты, средства контроля защищенности, средства управления событиями безопасности, средства защиты каналов передачи данных.

Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться сертифицированные на соответствие требованиям по безопасности средства защиты информации или средства, прошедшие оценку соответствия в форме испытаний или приемки в соответствии с Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

ГЛАВНОЕ

С начала 2018 года установка систем обеспечения безопасности инфраструктуры и обнаружения вторжений стала обязанностью всех госкомпаний, юридических лиц и индивидуальных предпринимателей, являющихся субъектами КИИ. Владельцы объектов КИИ должны информировать власти о компьютерных инцидентах и предотвращать попытки несанкционированного доступа к информации.

ЕДИНЫЙ РЕЕСТР РОССИЙСКИХ ПРОГРАММ

В соответствии с Постановлением Правительства РФ от 20.12.2017 № 1594 с 1 января 2018 года вступили в действие изменения в Постановление Правительства РФ от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

Новые требования к закупкам ПО для государственных и муниципальных нужд стали более жёсткими. В частности, запрещено не только прямое приобретение лицензий, но и аренда ПО, а также приобретение ПО, предустановленного на оборудовании.

Кроме того, расширен список случаев, в которых требуется сверяться с реестром российского ПО, а требования к включаемому в реестр софту стали более строгими.

ГЛАВНОЕ

При закупках ПО для государственных и муниципальных нужд заказчики обязаны приобретать только российские разработки, за исключением случаев, когда решения с необходимыми характеристиками отсутствуют в России. Это касается в том числе предустановленных и «облачных» программ.

Многофункциональный межсетевой экран и система обнаружения (предотвращения) вторжений Traffic Inspector и универсальный шлюз безопасности (UTM) и система обнаружения (предотвращения) вторжений Traffic Inspector Next Generation входят в Единый реестр российских программ.

Организация безопасного интернет-доступа в госструктурах

Организация безопасного интернет-доступа в госструктуре должна обеспечивать решение следующих задач:

1. Комплексную и качественную информационную безопасность.

2. Соблюдение российского законодательства в части:
   - запрета доступа к сайтам, включённым в реестр блокировок Роскомнадзора в соответствии с Законом № 149-ФЗ;
   - защиты персональных данных в соответствии с Законом № 152-ФЗ;
   - использования ПО, входящего в Единый реестр российских программ в соответствии с Постановлением Правительства РФ № 1236 и изменениями в Законе № 44-ФЗ.

3. Исключение рисков, связанных с резким изменением стоимости решения информационной безопасности, например из-за резких колебаний курса иностранной валюты.

РЕШЕНИЕ

Многофункциональный межсетевой экран и система обнаружения (предотвращения) вторжений Traffic Inspector и универсальный шлюз безопасности (UTM) и система обнаружения (предотвращения) вторжений Traffic Inspector Next Generation идеально подходят государственным и муниципальным организациям. Оба продукта разработаны российской компанией ООО «Смарт-Софт», включены в реестр российских программ и имеют сертификаты ФСТЭК по новым требованиям. Это позволяет рассматривать их как альтернативу иностранному ПО в рамках программы импортозамещения технических средств информационной безопасности.

Компания «Смарт-Софт» с 2003 года разрабатывает корпоративные системы защиты информации и управления интернет-доступом. Собственные разработки «Смарт-Софт» на основе уникальных запатентованных программных алгоритмов полностью соответствуют требованиям российского законодательства в области защиты информации и имеют все необходимые лицензии и сертификаты.

РЕКОМЕНДАЦИИ ГОСУДАРСТВЕННЫХ СТРУКТУР

Многофункциональный межсетевой экран и систему обнаружения (предотвращения) вторжений 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».

СЕРТИФИКАЦИЯ ФСТЭК

Компания «Смарт-Софт» лицензирована Федеральной службой по техническому и экспортному контролю (ФСТЭК) на деятельность по разработке и производству средств защиты конфиденциальной информации.

Сертифицированный многофункциональный межсетевой экран Traffic Inspector FSTEC имеет сертификат соответствия ФСТЭК России № 2407 от 15.08.2011 г., удостоверяющий, что ПО является межсетевым экраном типа Б и соответствует требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016) и «Профиль защиты межсетевых экранов типа Б пятого класса защиты. ИТ.МЭ.Б5.ПЗ» (ФСТЭК России, 2016). Срок действия сертификата – до 15.08.2020 г.

Сертифицированный универсальный шлюз безопасности (UTM) Traffic Inspector Next Generation FSTEC имеет сертификат соответствия № 3834 от 04.12.2017, удостоверяющий, что программно-аппаратный комплекс является межсетевым экраном типа А и Б и соответствует требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016) и «Профиль защиты межсетевых экранов типа А и Б четвертого класса защиты» ИТ.МЭ.А4.ПЗ и ИТ.МЭ.Б4.ПЗ. Срок действия сертификата – до 04.12.2020 г.

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 2407

Выдан 15 августа 2011 г.
Действителен до 15 августа 2017 г.
Срок действия продлен до 15 августа 2020 г.

Настоящий сертификат удостоверяет, что **программный комплекс «Traffic Inspector 3.0»**, разработанный и производимый ООО «СМАРТ-СОФТ» в соответствии с техническими условиями ТУ 5015-005-13346898-16, функционирующий в средах операционных систем, указанных в формуляре 501590-005-13346898-16 ФО, является межсетевым экраном типа «Б», соответствует требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016) и «Профиль защиты межсетевых экранов типа «Б» пятого класса защиты. ИТ.МЭ.Б5.ПЗ» (ФСТЭК России, 2016).

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ОАО «Безопасность информационных технологий и компонентов» (аттестат аккредитации от 31.05.2003 № СЗИ RU.1190.Б032.056) – техническое заключение от 24.01.2011, экспертного заключения от 21.07.2011 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 26.04.2005 № СЗИ RU.840.А92.007) и результатов инспекционного контроля, проведенного испытательной лабораторией ОАО «Безопасность информационных технологий и компонентов» – технические заключения от 20.07.2012, 21.06.2014, и испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 15.09.2016 № СЗИ.RU.0001.01БИ00.Б010) – техническое заключение от 30.03.2017.

Заявитель: ООО «СМАРТ-СОФТ»
Адрес: 140408, Московская обл., г. Коломна, ул. Сапожковых, д. 15
Телефон: (495) 775-5991

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
15 августа 2011 г.

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3834

Выдан 4 декабря 2017 г.
Действителен до 4 декабря 2020 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс «Traffic Inspector Next Generation»** разработанный и производимый ООО «СМАРТ-СОФТ» в соответствии с техническими условиями ТУ 5015-003-13346898-16, является межсетевым экраном типа «А» и «Б», соответствует требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016) , «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016) при выполнении указаний по эксплуатации, приведенных в формуляре 501590-003-13346898-16 ФО.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 15.09.2016 № СЗИ RU.0001.01БИ00.Б010) - техническое заключение от 07.09.2017, экспертного заключения от 17.11.2017 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ООО «СМАРТ-СОФТ» (ИНН 5022032904)
Адрес: 140408, Московская обл., г. Коломна, ул. Сапожковых, д. 15
Телефон: (495) 775-5991

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В. Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
4 декабря 2017 г.

СНИЖЕНИЕ РИСКОВ

Использование иностранного ПО в условиях санкций несёт серьёзную угрозу, поскольку вендор в любой момент может заблокировать или отключить лицензионные ключи, деактивировать часть функций либо полностью вывести из строя софт и оборудование с помощью заранее внедрённых «закладок». Результатом может стать полная остановка работы организации, что неприемлемо для обычных организаций и совершенно недопустимо для объектов критической информационной инфраструктуры.

Использование многофункционального межсетевого экрана и системы обнаружения (предотвращения) вторжений Traffic Inspector и универсального шлюза безопасности (UTM) и системы обнаружения (предотвращения) вторжений Traffic Inspector Next Generation позволяет исключить эти риски.

СТАБИЛЬНАЯ СТОИМОСТЬ

Цена за лицензию программного обеспечения не привязана к курсу валют. По договоренности можно закрепить стоимость для ожидания поступления бюджетных средств.

Функциональные возможности Traffic Inspector и Traffic Inspector Next Generation

Функционал	Traffic Inspector	Traffic Inspector Next Generation
Управление	Оснастка Microsoft Management Console поддержка централизованной системы управления	Веб-интерфейс, командная строка (SSH) поддержка централизованной системы управления
Протоколы	IPv4	IPv4, IPv6
Поддержка сетевых технологий	IEEE 802.3 (Ethernet) IEEE 802.11 (Wi-Fi) PPP IEEE 802.1Q VLAN Dial-Up Serial networking ISDN xDSL	IEEE 802.3 (Ethernet) PPP IEEE 802.1Q VLAN IEEE 802.1ad (QinQ)
Поддержка VPN	Виды VPN, поддерживаемые в ОС Windows (PPTP, L2TP/IPsec, IKEv2, SSTP) Туннели PPPoE	OpenVPN IPsec L2TP L2TP/IPsec PPTP Tinc VPN Туннели PPPoE, GIF, GRE

Преобразование сетевых адресов	RRAS NAT (Windows), ICS NAT (Windows) преобразований типа «один ко многим» (NAPT), преобразования «множество во множество» с возможной поддержкой взаимно однозначных преобразований (один к одному), проброс портов	PACKET FILTER NAT преобразований типа «один ко многим» (Pure NAT, NAPT), преобразования «множество во множество» с возможной поддержкой взаимно однозначных преобразований (один к одному), проброс портов
Типы пользователей	Пользователь, группа пользователей	600 Мбит/с при передаче IMIX-трафика
Рекомендуемое максимальное число клиентов	до 300 пользователей при работе через веб-прокси, до 1000 пользователей при работе в режиме маршрутизация по условию (решение о маршрутизации может приниматься на основе информации о сетевом протоколе, выходном интерфейсе, расписании и т. д.) NAT	Рекомендованное количество пользователей – до 100 для устройства S 100 Рекомендованное количество пользователей – до 1000 для устройства M 1000 Рекомендованное количество пользователей – свыше 1000 для устройства L 1000+
Аутентификация пользователей	Аутентификация по базам: локальная база пользователей, каталог Active Directory Аутентификация с помощью: HTTP Basic, HTTP NTLM, проприетарный протокол Аутентификация по IP/MAC/VLAN ID Идентификация пользователя в публичной сети по СМС и через ЕСИА Смешанная аутентификация (логин/пароль + привязка к IP/MAC-адресу)	Аутентификация по базам: локальная база пользователей, каталог Active Directory, RADIUS-сервер Аутентификация с помощью: HTTP Basic, HTTP NTLM, Kerberos, LDAP, RADIUS Аутентификация по IP-адресам Смешанная аутентификация (логин/пароль + привязка к IP/MAC-адресу) Идентификация пользователя в публичной сети по СМС Двухфакторная аутентификация по локальной базе в Captive Portal, на веб-прокси сервере и VPN-серверах
Защита сети	Контекстный файрвол, настраивается с помощью правил Встроенные шлюзовые антивирусы для проверки веб-трафика и почтового трафика	Контекстный файрвол, настраивается с помощью правил Встроенный шлюзовый антивирус для проверки веб-трафика и почтового трафика

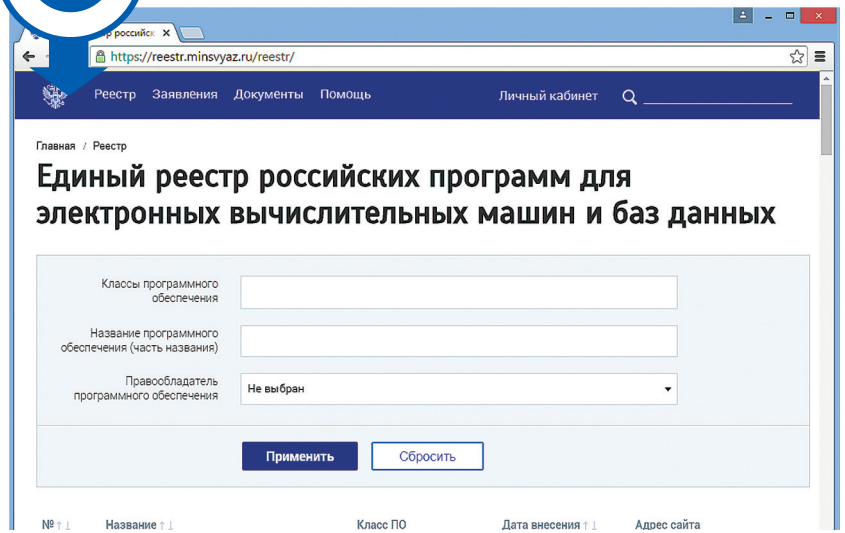
Защита сети		Поддержка интеграции с антивирусами по протоколу ICAP Система обнаружения/предотвращения вторжений Сканер сети GoLismero
Фильтрация	Фильтрация с помощью правил межсетевого экрана Фильтрация веб-трафика Контентная фильтрация с помощью NetPolice (сервис URL-категоризации) L7-фильтрация (nDPI) Декодирование и проверка HTTPS-трафика Почтовый шлюз и фильтрация спама	Фильтрация с помощью правил межсетевого экрана pf Фильтрация веб-трафика Контентная фильтрация с помощью NetPolice (сервис URL-категоризации) L7-фильтрация (nDPI) Декодирование и проверка HTTPS-трафика Почтовый шлюз и фильтрация спама
Управление трафиком	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 групп, приоритезация трафика Поддержка нескольких подключений к Интернету (Multi-WAN) Переключение на запасные интернет-каналы при выходе из строя основного канала (Connection Failover) Teaming/агрегация Ethernet-интерфейсов (в том числе IEEE 802.1AX) Бриджинг Ethernet-интерфейсов	Динамическая маршрутизация (OSPF, RIPv2 и BGPv4) Шейпер Поддержка нескольких подключений к Интернету (Multi-WAN) Переключение на запасные интернет-каналы при выходе из строя основного канала (Connection Failover) Teaming/агрегация Ethernet-интерфейсов (в том числе IEEE 802.1AX) Бриджинг Ethernet-интерфейсов Распределение входящей сетевой нагрузки между несколькими обслуживающими серверами во внутренней сети Балансировка исходящей нагрузки между несколькими WAN-подключениями Кластер высокой доступности

Прокси-серверы	Web-прокси SOCKS-прокси	Web-прокси Tor-proxy
Интеграция со службами каталогов	Microsoft Active Directory	Microsoft Active Directory Novell eDirectory OpenLDAP
Поддержка баз данных	Microsoft SQL Server, MySQL, PostgreSQL, SQLite	PostgreSQL
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	Отчет по сетевой активности на базе технологий NetFlow Отчеты по веб-прокси Отчеты и графики RRDtool Журнал сетевого экрана pf Системный журнал syslog

Как найти Traffic Inspector и Traffic Inspector Next Generation в Едином реестре российских программ для электронных вычислительных машин и баз данных

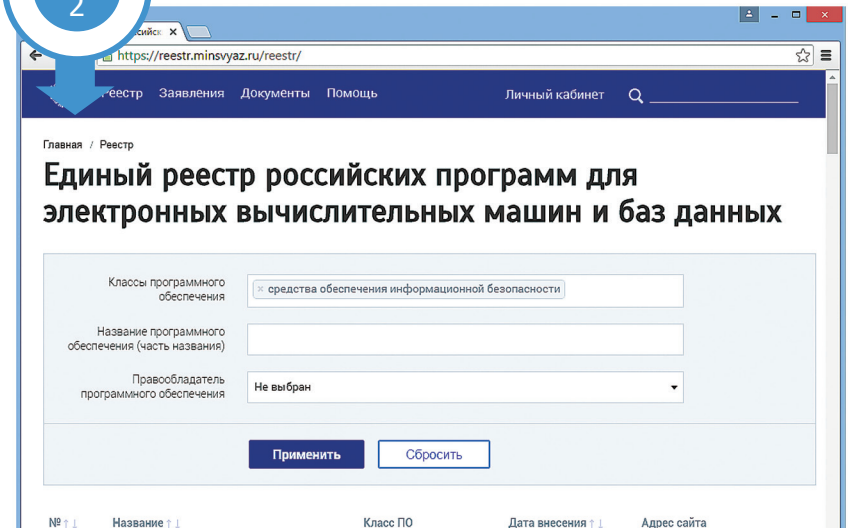
ШАГ 1

1. Зайти на сайт Единого реестра и выбрать класс программного обеспечения «Средства обеспечения информационной безопасности».



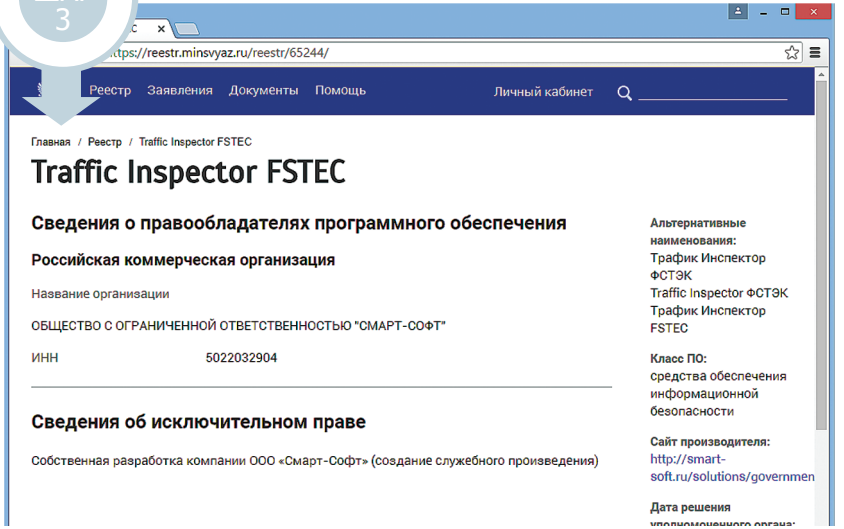
ШАГ 2

2. Указать в поле «Название программного обеспечения» «Traffic Inspector» и нажать «Применить».

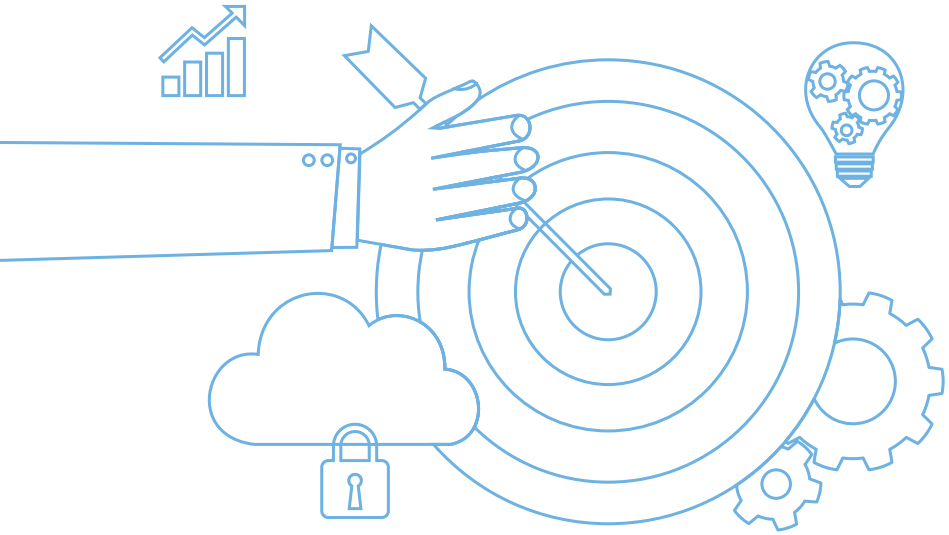


ШАГ 3

3. Нажмите на название продукта для просмотра информации о нём или перехода на сайт продукта.



Примеры успешного внедрения продуктов «Смарт-Софт» в госструктурах



ПРОКУРАТУРА МОСКВЫ

ЗАДАЧИ

1. Обеспечение информационной безопасности.
2. Контроль и учёт трафика.
3. Блокировка нежелательной рекламы, некоторых сайтов и спама.
4. Маршрутизация по условию.
5. Контентные фильтры.
6. Ограничение скорости работы в сети.

РЕШЕНИЕ

Для решения этих задач прокуратуре наилучшим образом подошел многофункциональный межсетевой экран и система обнаружения (предотвращения) вторжений Traffic Inspector. Он обеспечил качественный контроль за сетевым трафиком и всестороннюю информационную безопасность.

РЕЗУЛЬТАТ

Установка и настройка заняли всего несколько дней. Все возникшие в процессе внедрения вопросы были оперативно решены службой поддержки разработчика. На текущий момент Московская городская прокуратура использует Traffic Inspector более двух лет. Проблем с функционированием защитного решения не возникало.

МФЦ РЕСПУБЛИКИ ДАГЕСТАН

ЗАДАЧИ

1. Обеспечение информационной безопасности интернет-соединения для 57 филиалов и 345 удалённых офисов МФЦ.
2. Проксирование трафика.
3. Контроль интернет-трафика: мониторинг и статистика доступа.
4. Блокировка сайтов: правила по типам, группам и категориям.

РЕШЕНИЕ

По результатам изучения нескольких решений многофункциональный межсетевой экран и система обнаружения (предотвращения) вторжений Traffic Inspector оказался оптимальным в своем сегменте благодаря ценовой политике и индивидуальному подходу.

РЕЗУЛЬТАТ

После внедрения Traffic Incpector в филиалах МФЦ Республики Дагестан значительно снизилась нагрузка на каналы связи, и в кратчайшие сроки реализован комплексный контроль интернет-доступа.

УФНС РОССИИ ПО КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКЕ

ЗАДАЧИ

1. Разделить пользовательский и служебный трафик для 100 рабочих мест сотрудников УФНС.
2. Прекратить бесконтрольные утечки трафика.
3. Равномерно распределить нагрузку канала.
4. Обеспечить возможность гибкого управления интернет-доступом.

РЕШЕНИЕ

По итогам анализа рынка существующих проектов был выбран многофункциональный межсетевой экран и система обнаружения (предотвращения) вторжений Traffic Inspector. Этот проект является исключительно российской разработкой, представляет собой комплексное сертифицированное сетевое решение для организации и контроля доступа в Интернет и обладает полным набором функций, необходимых для учреждения. Программный продукт динамично развивается и имеет множество положительных отзывов.

РЕЗУЛЬТАТ

Внедрение Traffic Inspector в УФНС России по КБР обеспечило комплексное управление трафиком и максимально эффективное использование канала доступа в Интернет. Удобный интерфейс позволяет администраторам легко вносить изменения в настройки, а удобная система отчётов – анализировать расход трафика.

АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ г. ГУБКИНСКИЙ (ЯМАЛО-НЕНЕЦКИЙ АВТОНОМНЫЙ ОКРУГ)

ЗАДАЧИ

1. Заменить устаревшее защитное решение иностранного производства на более современное и функциональное.
2. Обеспечить безопасный доступ в Интернет для всех бюджетных учреждений и организаций города.
3. Повысить уровень защиты информации в сети.

РЕШЕНИЕ

Для выбора решения был проведён аукцион на поставку средств защиты информации в соответствии с Федеральным законом № 44-ФЗ «О контрактной системе». Обязательным конкурсным требованием было наличие у программного комплекса сертификата ФСТЭК, подтверждающего, что использование данного софта безопасно. Благодаря конкурентоспособной

цене, российскому происхождению и наличию сертификации победителем конкурса стал межсетевой экран и система обнаружения (предотвращения) вторжений Traffic Inspector.

РЕЗУЛЬТАТ

Приобретение файрвола стало одной из ступеней повышения уровня защиты информации, в рамках которого все бюджетные учреждения и организации города объединили в единую сеть с безопасным доступом в Интернет. Приятным бонусом стала возможность прямого контакта с разработчиком и обсуждение добавления новых функций в продукт. С прежним решением такое было невозможно в принципе.

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ АДЫГЕЯ

ЗАДАЧИ

1. Обеспечить выполнение требований Федерального закона №149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Обеспечить учет интернет-трафика и возможность составления отчетов.

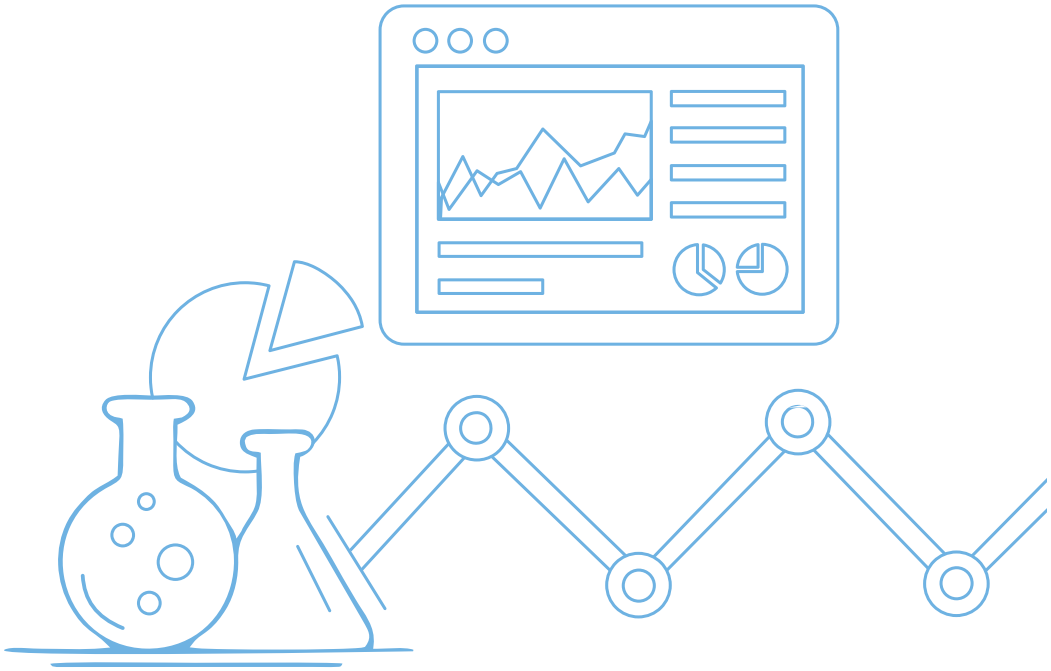
РЕШЕНИЕ

В отличие от коммерческих организаций, государственные заведения обязаны использовать программное обеспечение, имеющее сертификат ФСТЭК. Российских производителей подобного программного обеспечения немного. Сертифицированный многофункциональный межсетевой экран Traffic Inspector FSTEC оптимально подошел под требования и задачи министерства.

РЕЗУЛЬТАТ

Внедрение Traffic Inspector FSTEC заняло один рабочий день. Теперь компьютерная сеть министерства находится под надежной защитой Traffic Inspector FSTEC и в полном соответствии с российским законодательством.

Опыт использования продуктов «Смарт-Софт» в госструктурах



АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ пос. УРЕНГОЙ, ЯМАЛО-НЕНЕЦКИЙ АВТОНОМНЫЙ ОКРУГ

Использует межсетевой экран и систему обнаружения (предотвращения) вторжений Traffic Inspector с 2008 года. Продукт был выбран из-за привлекательной для бюджетной организации цены и качественной обратной связи с разработчиком. Приобретение иностранного ПО не рассматривали из-за невозможности получить сопоставимый с российским уровень техподдержки.

За время использования программным комплексом не было ни одного факта несанкционированного доступа к сети организации. Благодаря стабильной работе Traffic Inspector техподдержка потребовалась всего дважды в процессе перехода на новую версию файрвола.

В процессе эксплуатации у организации появились предложения по доработке ПО, связанные с удобством работы. После передачи предложений в техподдержку пожелания клиента были рассмотрены и поставлены в план перспективных доработок.

АДМИНИСТРАЦИЯ ЕМЕЛЬЯНОВСКОГО РАЙОНА, КРАСНОЯРСКИЙ КРАЙ

Опыт использования межсетевого экрана и системы обнаружения (предотвращения) вторжений Traffic Inspector – более 10 лет. Увидев файрвол в реальной эксплуатации в районном управлении образования, заинтересовались, а затем приобрели по доступной для бюджетной организации цене.

Использовать зарубежное ПО для защиты опасались, поскольку не было уверенности в том, что разработчики не оставили «закладок» или «черных ходов». К отечественному софту доверия больше, особенно при наличии сертификатов ФСБ и ФСТЭК.

Traffic Inspector обеспечивает организацию защиту от вторжения на серверы и несанкционированного доступа. Даже если кто-то из сотрудников попытается подключиться к сети со своим ноутбуком, файрвол не пропустит его трафик в сеть. Востребованной оказалась возможность контроля сетевой активности сотрудников и ограничения доступа к непрофильным ресурсам.

Отзывы о работе продуктов «Смарт-Софт» в госструктурах

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

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

– Я остановил свой выбор на Traffic Inspector. Этот комплексный продукт в области сетевой безопасности полностью удовлетворил наши ожидания и требования. Удобный интерфейс помогает нашим администраторам легко справляться с управлением системой. Доступная система отчетов позволяет анализировать весь расход трафика.
Помимо привлекательной для бюджетной организации цены, мне понравилось, что команда специалистов компании готова оперативно отвечать и помогать разрешать мои вопросы.

Марат Гасанов,
директор по информационной безопасности МФЦ Республики Дагестан

– Согласно отзывам IT-специалистов СГУ, именно стабильность ПО является одним из самых важных показателей, благодаря которым работа по обеспечению информационной безопасности и обеспечению научным контентом ведется на самом высоком уровне. Этим Traffic Inspector в лучшую сторону отличается от прочих биллинговых систем.

ФБГОУ ВО «Сочинский государственный университет»

– 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

О КОМПАНИИ

Компания «Смарт-Софт» сегодня – это:

15 ЛЕТ

На рынке систем информационной безопасности с 2003 г.

2 АССОЦИАЦИИ

Членство в двух ведущих ассоциациях АРПП «Отечественный софт» и «Руссофт».

ГЕОГРАФИЯ ПРИСУТСТВИЯ

Широкая география присутствия продуктов компании в России и странах СНГ.

КОНТАКТЫ

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