ГОСУДАРСТВЕННЫЕ СТРУКТУРЫ

Методическое пособие
по информационной безопасности

Советы по
IT-безопасности
внутри

SMART-SOFT

Фото: Михаил Метцель, ТАСС

...мы реализуем в России программу конкретных мер по борьбе с киберпреступлениями... будем стремиться, чтобы действующие в России программное обеспечение и инфраструктура связи основывались на отечественных технологиях и решениях, которые прошли соответствующую проверку и сертификацию, — конечно, не в ущерб конкуренции: само собой разумеется, речь идет о конкурентоспособных продуктах, соответствующих самым высоким запросам потребителей.

Источник: http://kremlin.ru/events/president/news/57957

Считаю, что нужно усилить персональную ответственность руководителей для обеспечения информационной безопасности.

Источник: https://www.interfax.ru/russia/584679

Президент РФ Владимир Путин

Общая ситуация на рынке

Удорожание зарубежной продукции

В результате падения курса рубля относительно основных иностранных валют снизило ее конкурентоспособность.

Введение антироссийских санкций

Затруднило использование иностранного программного обеспечения (ПО) многими секторами российской экономики.

Принятие законов об иностранном ПО

Наложило ограничения на закупку зарубежного софта государственными и муниципальными организациями, а также компаниями с государственным участием.

Проведение «цифровых» законов

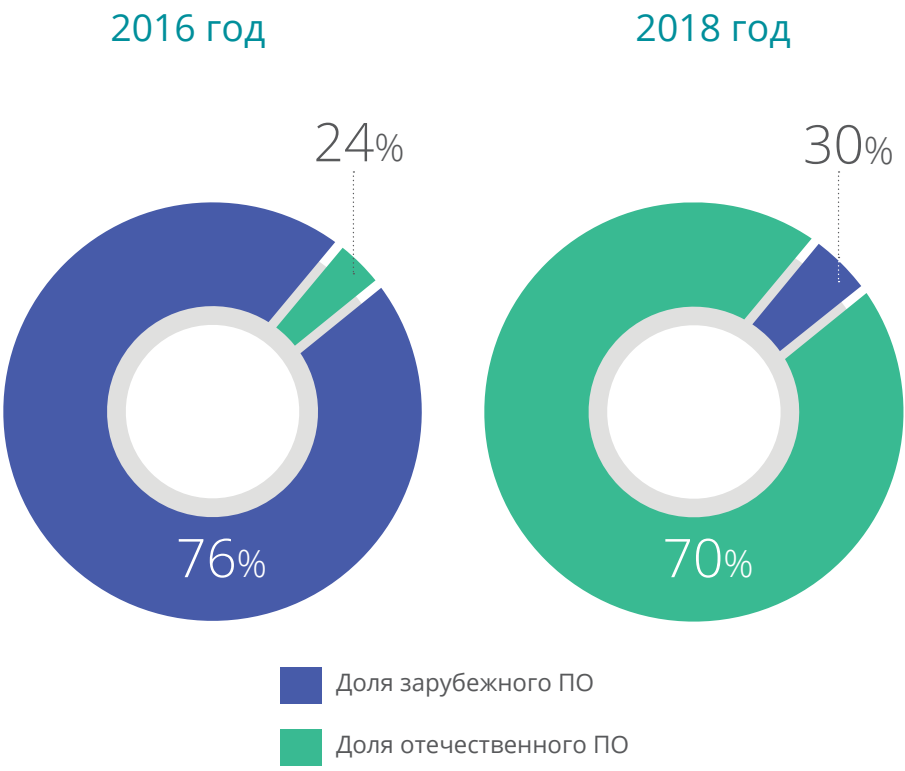
Усилило персональную ответственность руководителей организаций, работающих с персональными данными, компаний, входящих в критическую информационную инфраструктуру РФ, и учреждений, обязанных блокировать сайты с запрещенной информацией.

Усиление мер поддержки отечественных разработчиков ПО

Привело к созданию единого реестра российских программ и Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий.

Доля российского программного обеспечения в закупках госорганами в 2018 году достигла 70%.

Источник: «Парламентская газета».

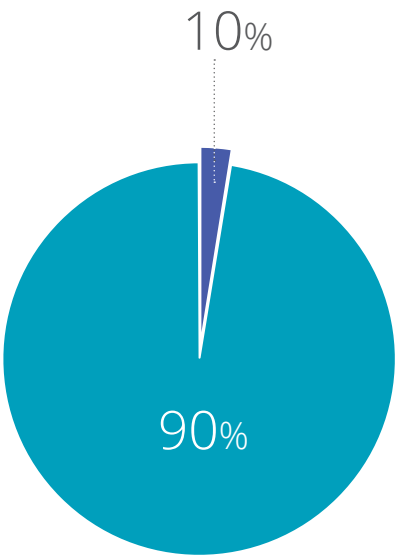


Согласно паспорту национальной программы «Цифровая экономика», в течение шести лет доля российского программного продукта в государственных структурах должна увеличиваться каждый год на 5%.

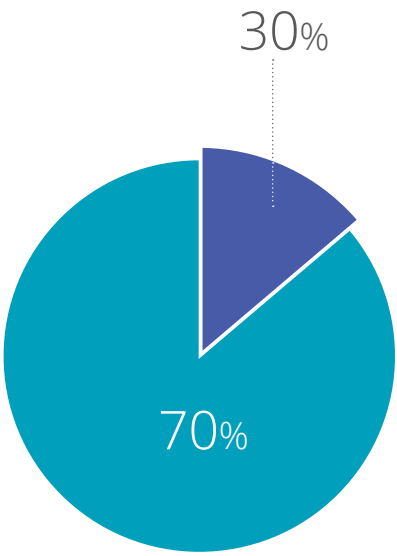
Источник: http://d-russia.ru/soveshhanie-u-premer-ministra-po-povodu-otechestvennogo-po-podrobnosti.html

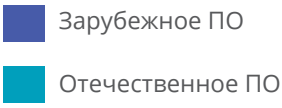
ДОЛЯ ЗАКУПАЕМОГО И (ИЛИ) АРЕНДУЕМОГО ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В 2024 ГОДУ (ПЛАН)

Для федеральных органов исполнительной власти, органов исполнительной власти субъектов и иных органов государственной власти

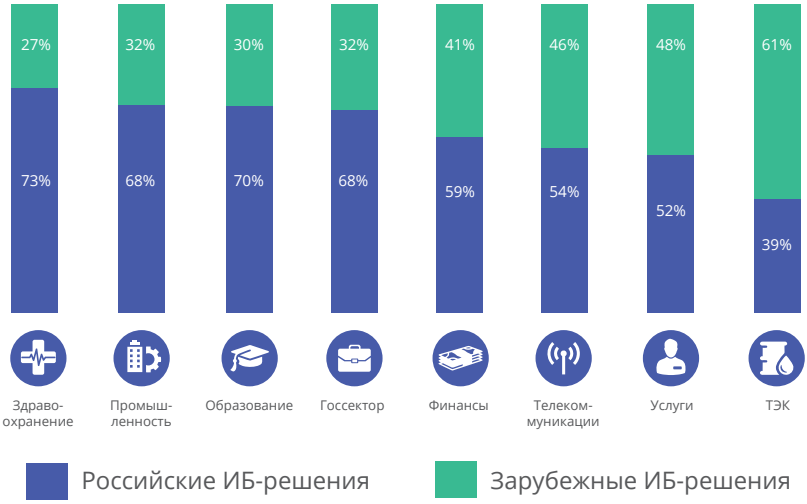


Для компаний с государственным участием

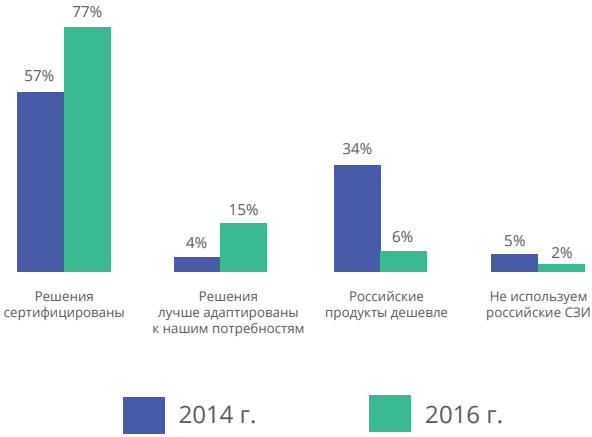




СООТНОШЕНИЕ РОССИЙСКИХ И ЗАРУБЕЖНЫХ РЕШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАЗЛИЧНЫХ ОТРАСЛЯХ (НА 2017 ГОД)



ФАКТОРЫ ВЫБОРА ОТЕЧЕСТВЕННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



Источник: https://www.securitycode.ru/upload/Importozameschenie_2017.pdf

СОВРЕМЕННЫЕ БЮДЖЕТНЫЕ ОРГАНИЗАЦИИ НУЖДАЮТСЯ В ЦИФРОВОЙ ЗАЩИТЕ НЕ МЕНЬШЕ, ЧЕМ КОММЕРЧЕСКИЕ

13% **всех хакерских атак было направлено на госсектор** в 2017 году, говорится в отчете Positive Technologies. Треть нападений произошла с целью получения данных (шпионажа). В атаках такого рода главной целью злоумышленников является получение доступа к внутренним ресурсам и защищаемой информации. Кроме того, получив доступ к серверам, злоумышленники могут делать все, что им вздумается: могут затаиться и ждать подходящего момента, а могут вывести из строя серверное оборудование или уничтожить базы данных.

Источник: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf

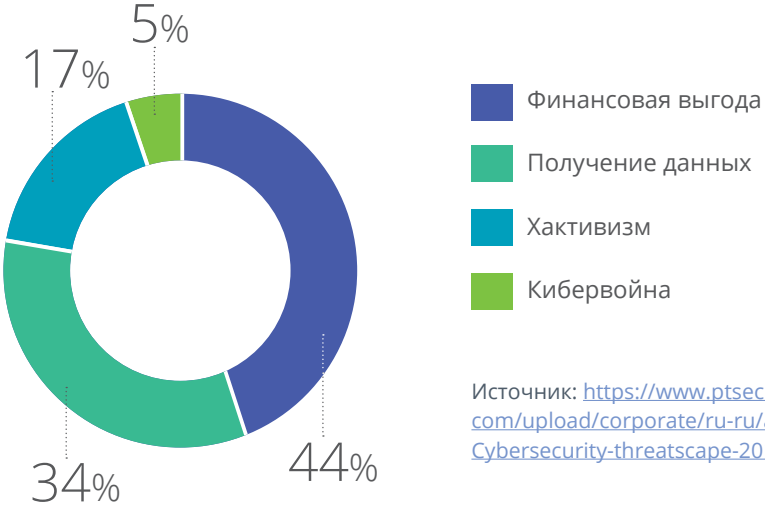
Фишинговые атаки теперь не ограничиваются банками, платежными системами, соцсетями. Эксперты «Лаборатории Касперского» подсчитали, что с сентября 2017 года по сентябрь 2018 года около 1000 фишинговых атак пришлось на сайты ведущих мировых университетов. Целью мошенников был сбор конфиденциальных данных, включая результаты научных исследований во множестве областей: от экономики до ядерной физики.

Источник: https://www.kaspersky.ru/about/press-releases/2018_pr-scholars-phishing

Кроме того, с помощью фишинга киберпреступники атаковали более 400 промышленных компаний, преимущественно на территории России. Цель — кража денежных средств со счетов организаций.

Источник: https://www.kaspersky.ru/about/press-releases/2018_industrial-companies-targeted-with-spear-fishing

МОТИВЫ АТАК НА ГОСПРЕДПРИЯТИЯ



Источник: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf

ПРОЦЕНТ АТАКОВАННЫХ КОМПЬЮТЕРОВ АСУ В РАЗЛИЧНЫХ ИНДУСТРИЯХ, ПЕРВОЕ И ВТОРОЕ ПОЛУГОДИЯ 2017 ГОДА

Среди лидеров роста интереса хакеров — образование, энергетика, разработка промышленного ПО.

Источник: https://ics-cert.kaspersky.ru/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017/

Интернет и законодательство

ЗАПРЕТ ИНОСТРАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Постановление № 1236 от 16 ноября 2015 года ограничивает закупки иностранного ПО для государственных и муниципальных нужд. Оно вступило в действие одновременно с запуском Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий и Единого реестра российских программ для ЭВМ и баз данных. Заказчикам реестр помогает находить замену иностранным решениям, а производителям выходить на рынок, не имея огромных рекламных бюджетов, которыми располагают западные вендоры.

Источник: http://static.government.ru/media/files/ac872y0wqioFnrRUeTnpGjEavWCfgEAo.pdf

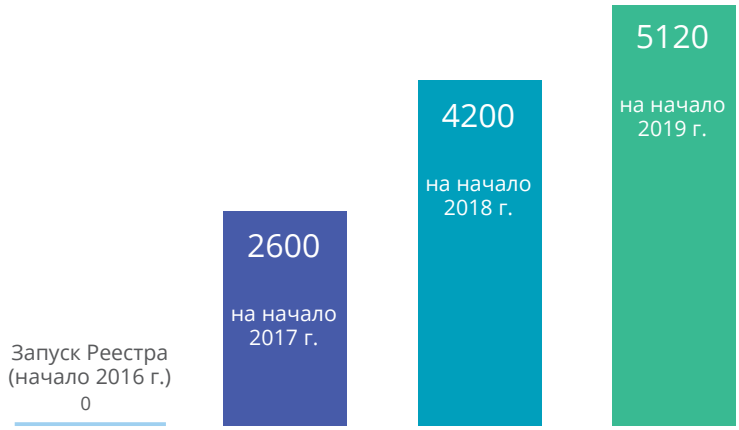
С 1 января 2018 года требования относительно иностранного ПО стали более жесткими. В частности, согласно Постановлению Правительства РФ от 20.12.2017 No 1594 (о внесении изменений в Постановление № 1236), запрещено не только прямое приобретение лицензий, но и аренда ПО, а также приобретение софта, предустановленного на оборудовании.

В Единый реестр российских программ для ЭВМ и баз данных входят решения «Смарт-Софт»:

– Traffic Inspector FSTEC;

– Traffic Inspector Next Generation FSTEC .

КОЛИЧЕСТВО РАЗРАБОТОК ОТЕЧЕСТВЕННОГО ПО В ЕДИНОМ РЕЕСТРЕ РОССИЙСКИХ ПРОГРАММ ДЛЯ ЭВМ И БАЗ ДАННЫХ



Источник: https://reestr.minsvyaz.ru/reestr/

ЗАКОН О БЛОКИРОВКЕ САЙТОВ

Закон № 149-ФЗ «Об информации, информационных технологиях и защите информации» вводит понятие **реестра сайтов**, содержащих запрещенную в РФ информацию. Согласно закону, доступ к сайтам, включенным 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 решения: сертифицированный многофункциональный межсетевой экран **Traffic Inspector FSTEC** и сертифицированный универсальный шлюз безопасности (UTM) **Traffic Inspector Next Generation FSTEC**, входящие в Единый реестр российских программ для ЭВМ и баз данных.

Что относится к запрещенной информации:

- детская порнография, сведения о наркотиках, самоубийствах, азартных играх и несчастных случаях с несовершеннолетними;
- фильмы, книги, фотографии, музыка и другая информация, защищенная авторскими правами;
- призывы к насилию, экстремизму и массовым беспорядкам.

ЗАКОН О ПЕРСОНАЛЬНЫХ ДАННЫХ

Закон № 152-ФЗ определяет порядок работы с информацией, прямо или косвенно относящейся к физическому лицу. Одно из требований закона — защита персональных данных физических лиц (сотрудников, клиентов, посетителей и т. д.). Защита персональных данных включена в раздел охраны труда на предприятии (государство гарантирует их защиту всем работникам).

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.

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.

Обеспечить защиту информационных систем в соответствии с законодательством РФ помогут решения **Traffic Inspector FSTEC** и **Traffic Inspector Next Generation FSTEC**, прошедшие сертификацию на соответствие требованиям ФСТЭК России к межсетевым экранам.

Завершение сертификации антивирусной защиты и системы обнаружения (предотвращения) вторжений планируется в первом полугодии 2019 года.

ЗАКОН О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РФ

Согласно Федеральному закону от 26.07.2017 года № 187-ФЗ, 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.

Закон накладывает ряд обязанностей на организации и компании, относящиеся к субъектам КИИ, в числе которых:
– соблюдение требований по обеспечению безопасности;
– незамедлительная реакция на компьютерные инциденты;
– оповещение уполномоченных организаций.

К программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ, относятся в том числе средства защиты информации от несанкционированного доступа, межсетевые экраны, средства обнаружения и предотвращения вторжений,

Кто является субъектом КИИ?

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 финансового 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.

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 средства защиты информации или средства, прошедшие оценку соответствия в форме испытаний или приемки.

Источник: https://fstec.ru/normotvorcheskaya/akty/53prikazy/1589prikazfstekrossiiot21dekabrya2017gn236

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.
Нарушение законов ведет к негативным последствиям, вплоть до штрафов и персонального взыскания с руководителя организации. Избежать этого можно с помощью одного решения — так называемой UTM-системы.

Установив UTM-решение, отвечающее требованиям законодательства, руководитель может быть уверен в том, что в его организации не нарушается ни один федеральный закон.

При выборе UTM-решения руководитель организации должен учесть следующее:

- российские разработчики лучше иностранных разбираются в нюансах законодательства РФ, под которое подстраивают функциональность своих решений;
- отечественные производители софта не откажут в поддержке из-за санкций (в отличие от западных - источник: https://www.vedomosti.ru/technology/articles/2018/05/28/770886-akado-cisco), при этом российские решения, как правило, доступнее по цене;
- Федеральная служба по техническому и экспортному контролю (ФСТЭК) требует от государственных организаций наличия соответствующего сертификата на используемое ПО.

ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННОМ СЕКТОРЕ И ИХ РЕШЕНИЯ

	Задачи	Решения
 Все государственные структуры и госкорпорации	Постановлением № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств...» определено, что госучреждения должны использовать российское программное обеспечение, а также утверждены правила формирования и ведения Единого реестра российских программ для ЭВМ и баз данных. Приказом ФСТЭК России № 17 от 11.02.2013 утверждены Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Согласно требованиям, для обеспечения защиты такой информации должны применяться средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации (т.е. имеющие соответствующий сертификат ФСТЭК). Закон «О безопасности критической информационной инфраструктуры...» (№ 187-ФЗ) обязывает организации, подпадающие под приведенный в нем перечень отраслей, информировать об инцидентах информационной безопасности уполномоченный орган.	Решения Traffic Inspector FSTEC и Traffic Inspector Next Generation FSTEC входят в Единый реестр российских программ для ЭВМ и баз данных и имеют сертификаты соответствия ФСТЭК России (Traffic Inspector FSTEC — сертификат № 2407 от 15.08.2011 года, действителен до 15.08.2020 года, Traffic Inspector Next Generation FSTEC — сертификат № 3834 от 04.12.2017 года, действителен до 04.12.2020 года). Завершение сертификации антивирусной защиты и системы обнаружения (предотвращения) вторжений планируется в первом полугодии 2019 года. Решения способны обнаруживать и предупреждать хакерские атаки, а также фиксировать действия злоумышленников для содействия в расследовании этих инцидентов.

 Учебные заведения	В местах, доступных для детей, организатор доступа в интернет обязан обеспечить информационную безопасность детей, применяя административные и организационные меры, технические и программно-аппаратные средства защиты детей от информации, причиняющей вред их здоровью и развитию (Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» № 436-ФЗ, Приказ Минкомсвязи России № 161 от 16.06.2014 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей...»). В частности, должен быть заблокирован доступ к информации, провоцирующей на суицид, употребление наркотических средств, побуждающей к жестокости, пропагандирующей нетрадиционные сексуальные отношения, содержащей нецензурную брань, порнографию и др. За несоблюдение этих требований как руководитель, так и сама образовательная организация могут быть оштрафованы контролирующими органами.	В настройках межсетевого экрана есть опция блокировки отдельных групп в соцсетях и разделов сайтов. Вместе с тем разрешенный контент порталов остается доступным, если это необходимо для учебного процесса (например, в «Википедии» можно заблокировать статьи о том, как создавать запрещенные вещества в домашних условиях, но оставить доступ к полезным статьям). Подключение к порталу Роскомнадзора позволяет скачивать оттуда реестр сайтов из черного списка в режиме реального времени. Модуль контентной фильтрации определяет и блокирует «плохие» страницы по содержащимся на них словам. Администратор может использовать уже готовые списки, дополнять их или составлять свои.

 Организации здравоохранения	Современные учреждения здравоохранения имеют разветвленную филиальную сеть и активно взаимодействуют друг с другом по открытым интернет-каналам. В данных, которыми обмениваются медицинские учреждения, содержится конфиденциальная информация о пациентах, истории их болезни, а также персональная информация о медицинских работниках. Утечка такой информации грозит нарушением закона «О защите персональных данных» (№ 152-ФЗ).	Технология шифрования данных VPN (Virtual Private Network) полностью исключает возможность перехвата информации, передаваемой между медицинскими учреждениями. Система IDS/IPS для обнаружения и предотвращения неавторизованного доступа и другие современные средства защиты отражают различные типы атак.
 Учреждения культуры и досуга (музеи, библиотеки, театры)	Оказание универсальных услуг связи по передаче данных и предоставлению доступа в интернет с использованием пунктов коллективного доступа может осуществляться оператором универсального обслуживания только после идентификации пользователей (Постановление Правительства РФ № 758 от 31 июля 2014 г. «О внесении изменений в некоторые акты Правительства Российской Федерации...») Источник: https://rg.ru/2014/08/05/svyaz-site-dok.html	Для авторизации посетителей используется SMS-идентификация по номеру телефона его владельца. После того как пользователь подключается к Wi-Fi, он попадает на специальную страницу, вводит номер своего телефона, получает сообщение с кодом доступа, вводит его на следующей странице и получает доступ в сеть.

Почему государственные структуры выбирают решения «Смарт-Софт»

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

Многофункциональный межсетевой экран Traffic Inspector FSTEC имеет сертификат соответствия ФСТЭК России № 2407 от 15.08.2011 года, 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 года.

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

Завершение сертификации антивирусной защиты и системы обнаружения (предотвращения) вторжений планируется в первом полугодии 2019 года.

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.A92.007) 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.A002).

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.

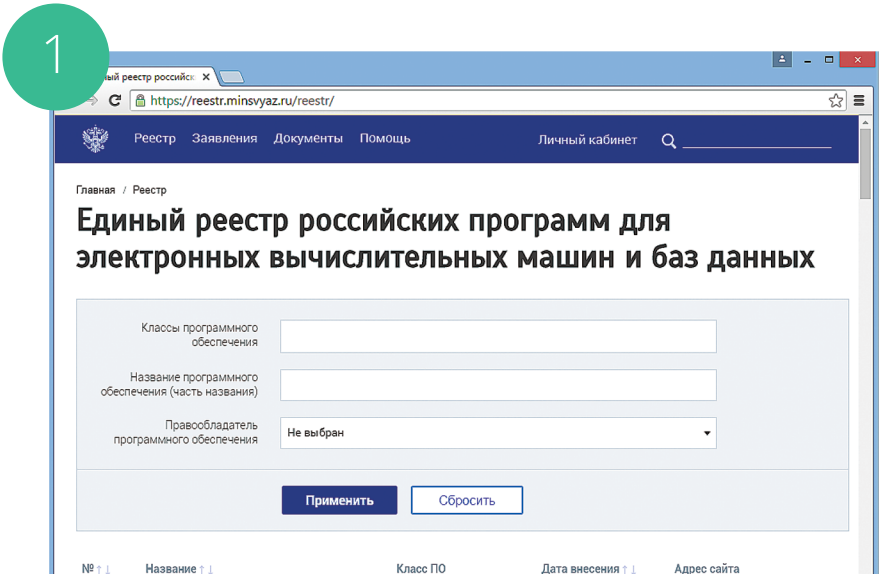
Traffic Inspector и Traffic Inspector Next Generation занесены в Единый реестр российских программ для электронных вычислительных машин и баз данных.

Как найти решения «Смарт-Софт» в реестре:

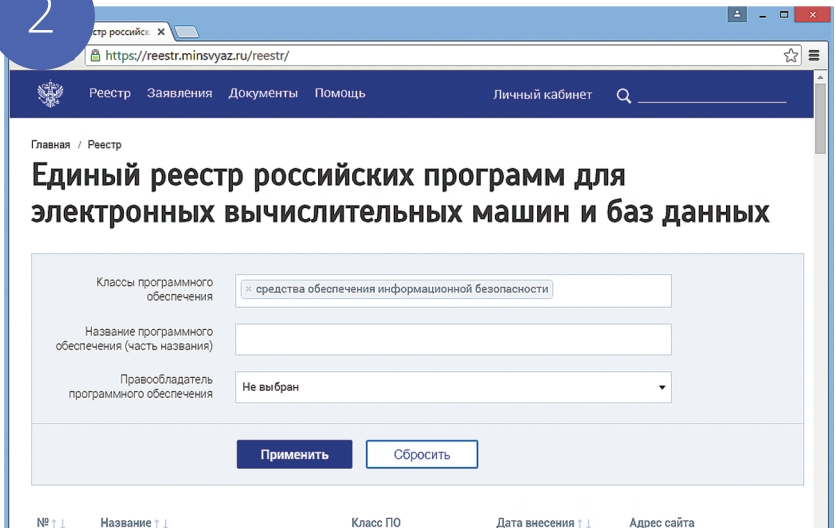
1. Зайти на сайт Единого реестра: https://reestr.minsvyaz.ru/reestr/

2. В строку поиска ввести название нужного продукта (Traffic Inspector или Traffic Inspector Next Generation).

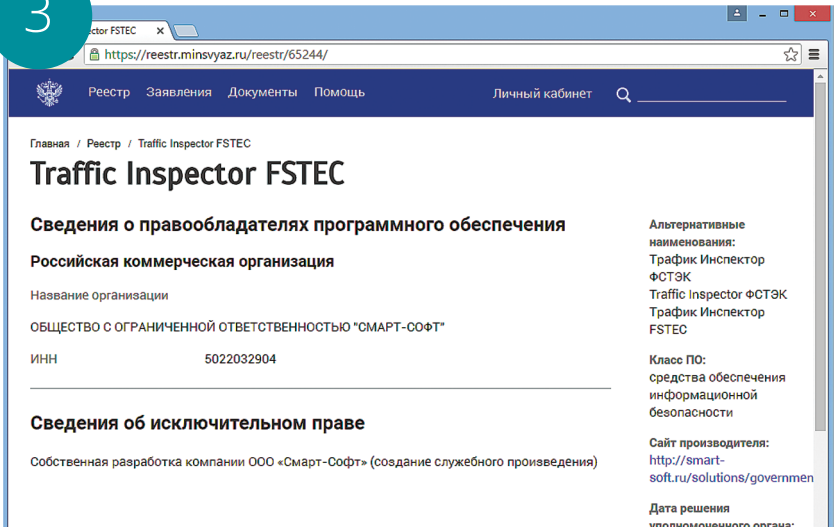
3. Вместо названия можно использовать общие слова: «межсетевой экран», «универсальный шлюз», «шлюз безопасности», «система обнаружения вторжений».



2


https://reestr.minsvyaz.ru/reestr/
Реестр
Заявления
Документы
Помощь
Личный кабинет
Главная / Реестр
Единый реестр российских программ для электронных вычислительных машин и баз данных
Классы программного обеспечения
средства обеспечения информационной безопасности
Название программного обеспечения (часть названия)
Правообладатель программного обеспечения
Не выбран
Применить
Сбросить
№
Название
Класс ПО
Дата внесения
Адрес сайта

3


https://reestr.minsvyaz.ru/reestr/65244/
Реестр
Заявления
Документы
Помощь
Личный кабинет
Главная / Реестр / Traffic Inspector FSTEC
Traffic Inspector FSTEC
Сведения о правообладателях программного обеспечения
Российская коммерческая организация
Название организации
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "СМАРТ-СОФТ"
ИНН
5022032904
Сведения об исключительном праве
Собственная разработка компании ООО «Смарт-Софт» (создание служебного произведения)
Альтернативные наименования:
Трафик Инспектор ФСТЭК
Traffic Inspector ФСТЭК
Трафик Инспектор FSTEC
Класс ПО:
средства обеспечения информационной безопасности
Сайт производителя:
http://smart-soft.ru/solutions/governmen
Дата решения

Истории внедрения

ТЮМЕНСКИЙ МЕДУНИВЕРСИТЕТ

ЗАДАЧИ

Руководством высшего учебного заведения была поставлена задача обеспечить локальную сеть (500 компьютеров) единой точкой выхода в интернет, которая бы обеспечивала безопасное соединение и возможность блокировки доступа к сайтам. Мотивы руководства:

- сотрудники проводят много времени в социальных сетях, на сайтах знакомств и других нецелевых ресурсах;
- пользователи внутренней сети заходят на потенциально опасные внешние ресурсы;
- нецелевое использование интернета резко увеличило трафик, нагрузку на локальную сеть и расходы организации;
- растущая угроза хакерской атаки извне.

РЕШЕНИЕ

Программно-аппаратный комплекс Traffic Inspector Next Generation наилучшим образом подошел под требования заказчика, поскольку обладает сертификатом ФСТЭК и всеми необходимыми функциями.

РЕЗУЛЬТАТ

«Решение Traffic Inspector Next Generation FSTEC оказалось не только наиболее подходящим, но и самым выгодным: у конкурентов цена под нужное количество компьютеров оказалась выше в два-три раза!».

Франчук Тарас,
инженер отдела ИБ университета

УФНС РОССИИ ПО КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКЕ

ЗАДАЧИ

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

РЕШЕНИЕ

По итогам анализа рынка было выбрано решение Traffic Inspector. Эта российская разработка обладает полным набором функций, необходимых для учреждения.

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 отчетов — анализировать расход трафика.

«Хотелось бы поблагодарить менеджеров компании «Смарт-Софт», которые с вниманием и пониманием отнеслись к 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

ПРОКУРАТУРА МОСКВЫ

ЗАДАЧИ

- Обеспечение информационной безопасности.
- Контроль и учет трафика.
- Блокировка нежелательной рекламы, некоторых сайтов и спама.
- Маршрутизация по условию.
- Контентные фильтры.
- Ограничение скорости работы в сети.

РЕШЕНИЕ

Прокуратуре наилучшим образом подошел многофункциональный межсетевой экран Traffic Inspector. Внедрение обеспечило качественный контроль сетевого трафика и комплексную информационную безопасность.

РЕЗУЛЬТАТ

Установка и настройка заняли всего несколько дней. Любые возникавшие в процессе внедрения вопросы оперативно решались службой поддержки разработчика. На момент написания отзыва Московская городская прокуратура использовала Traffic Inspector более двух лет. Проблем с функционированием защитного решения не возникало.

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ АДЫГЕЯ

ЗАДАЧИ

- Обеспечить выполнение требований Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- 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.

АДМИНИСТРАЦИЯ ЕМЕЛЬЯНОВСКОГО РАЙОНА, КРАСНОЯРСКИЙ КРАЙ

Опыт использования многофункционального межсетевого экрана Traffic Inspector — более 10 лет. Увидев файрвол в реальной эксплуатации в районном управлении образования, заинтересовались, а затем приобрели по доступной для бюджетной организации цене.

РЕШЕНИЕ

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 сертификата ФСТЭК.

РЕЗУЛЬТАТ

Traffic Inspector обеспечивает организации защиту от вторжения на серверы и несанкционированного доступа. Востребованной оказалась возможность контроля сетевой активности сотрудников и ограничения доступа к непрофильным ресурсам.

АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ г. ГУБКИНСКИЙ, ЯМАЛО-НЕНЕЦКИЙ АВТОНОМНЫЙ ОКРУГ

ЗАДАЧИ

- Заменить устаревшее защитное решение иностранного производства на более современное и функциональное.
- Обеспечить безопасный доступ в интернет для всех бюджетных учреждений и организаций города.
- Повысить уровень защиты информации в Сети.

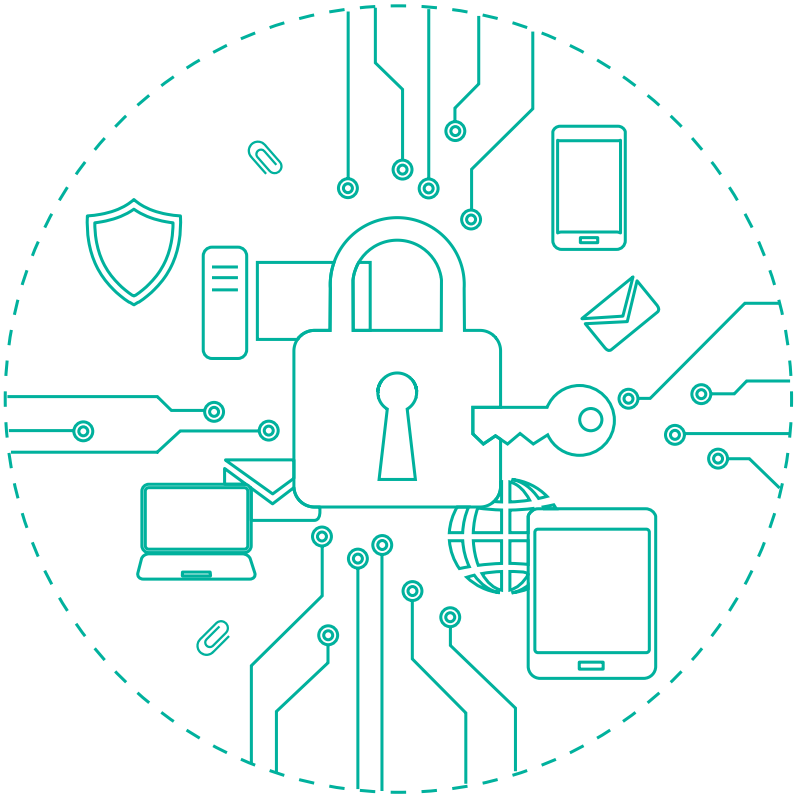
РЕШЕНИЕ

Для выбора решения был проведен 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 сертификата победителем конкурса стал сертифицированный многофункциональный межсетевой экран Traffic Inspector.

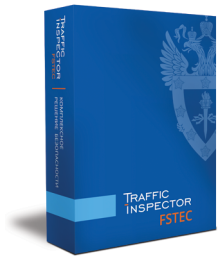
РЕЗУЛЬТАТ

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. Приятными бонусами стали возможность прямого контакта с разработчиком и обсуждение добавления новых функций в продукт. С прежним решением такое было невозможно в принципе.

Решения «Смарт-Софт»



TRAFFIC INSPECTOR FSTEC



Сертифицированный многофункциональный межсетевой экран

Программный комплекс

Количество учетных записей: от 5 до 500 (максимальное количество пользователей зависит от характера трафика и используемой настройки функциональных модулей).

ОС Windows.

Сертификат соответствия ФСТЭК России № 2407 от 15.08.2011 года.

Межсетевой экран типа «Б», соответствует требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016) .

TRAFFIC INSPECTOR NEXT GENERATION FSTEC

Сертифицированный универсальный шлюз безопасности (UTM)

Программно-аппаратный комплекс

Количество учетных записей: до 100 пользователей (S 100), от 100 до 500 пользователей (S 500), от 500 до 1000 (M 1000) и более 1000 пользователей (L 1000+).

ОС FreeBSD.

Сертификат соответствия ФСТЭК России № 3834 от 04.12.2017 года.

Программно-аппаратный комплекс является межсетевым экраном типа «А» и «Б» и соответствует требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016).

TRAFFIC INSPECTOR FSTEC

«Профиль защиты межсетевых экранов типа «Б» пятого класса защиты. ИТ.МЭ.Б5.ПЗ» (ФСТЭК России, 2016).

Срок действия сертификата — до 15.08.2020 года.

TRAFFIC INSPECTOR NEXT GENERATION FSTEC

«Профиль защиты межсетевых экранов типа «А» четвертого класса защиты. ИТ.МЭ.А4.ПЗ» и «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты. ИТ.МЭ.Б4.ПЗ».

Срок действия сертификата — до 04.12.2020 года.

Завершение сертификации антивирусной защиты и системы обнаружения (предотвращения) вторжений (IDS/IPS) планируется в первом полугодии 2019 года.

Где можно применять

– в государственных информационных системах второго класса защищенности (не работающих с государственной тайной);

– в автоматизированных системах управления производственными и технологическими процессами второго класса защищенности;

– в информационных системах персональных данных при необходимости обеспечения второго уровня защищенности персональных данных.

– в государственных информационных системах первого и второго класса защищенности;

– в автоматизированных системах управления производственными и технологическими процессами первого класса защищенности;

– в информационных системах персональных данных при необходимости обеспечения первого уровня защищенности персональных данных;

– в информационных системах общего пользования второго класса.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

		TRAFFIC INSPECTOR® FSTEC	TRAFFIC INSPECTOR NEXT GENERATION FSTEC
Краткое описание		Программный комплекс, который можно установить на уже имеющийся сервер или компьютер высокой производительности. Не требует приобретения дополнительного оборудования. Решение на базе ОС Windows.	Программно-аппаратный комплекс. В зависимости от количества сотрудников можно выбрать решения на 100, 500, 1000 и более лицензий. Решение на базе FreeBSD.
Защита от атак	Межсетевой экран (Firewall)	+	+
	VPN	+	+
	Proxy	+	+
	Система IDS/IPS	В процессе получения сертификата	
Фильтрация трафика и защита от нежелательного контента	Фильтрация с помощью правил межсетевого экрана	+	+
	Фильтрация веб-трафика	+	+
	Контентная фильтрация	Дополнительный модуль NetPolice	
	L7-фильтрация	+	+
	Декодирование и проверка HTTPS-трафика	+	+

		Traffic Inspector FSTEC	Traffic Inspector Next Generation FSTEC
Балансировка трафика	Шейпер (ограничение скорости работы пользователей и групп)	+	-
	Приоритизация трафика	+	+
	Переключение на запасные интернет-каналы (переключение происходит автоматически при выходе из строя основного канала)	+	+
	Бриджинг Ethernet-интерфейсов	-	+
	Распределение входящей сетевой нагрузки между несколькими обслуживающими серверами во внутренней сети	-	+
	Балансировка исходящей нагрузки между несколькими WAN-подключениями	-	+
	Кластер высокой доступности	-	+
Соблюдение «цифровых» законов РФ		Блокировка контента 18+ Защита персональных данных	Блокировка контента 18+ Защита персональных данных
Ведение учета посещаемости веб-ресурсов и активности в сети	Сетевая статистика	+	На базе технологий NetFlow
	Отчет по пользователям, отчет по времени, отчет по скорости, отчет по активности пользователей	+	Отчеты и графики RRDtool
	Отчет антивируса	+	+
	Отчет веб-прокси	+	+

		Traffic Inspector FSTEC	Traffic Inspector Next Generation FSTEC
Ведение учета посещаемости веб-ресурсов и активности в сети	Журнал действий системного администратора	+	+
	Журнал сетевого экрана (в том числе фиксация попыток несанкционированного доступа)	-	+
	Системный журнал FreeBSD	-	+
Количество пользователей		От 5 до 500 (максимальное количество пользователей зависит от характера трафика и используемой настройки функциональных модулей)	В зависимости от модификации: S 100 — до 100, S 500 — до 500, M 1000 — до 1000, L 1000+ — более 1000

5 ФАКТОВ О КОМПАНИИ «СМАРТ-СОФТ»

Российский разработчик

Разработка и техническая поддержка продуктов — в России.

Старше Facebook

Первые строчки кода разработчики «Смарт-Софт» написали в 2003 году.

1 975 лицензий

Максимальное количество лицензий, которое было приобретено одним заказчиком единовременно.

5 компьютеров

Самая маленькая локальная сеть, которую защищает решение от «Смарт-Софт».

Анадырь

Самый восточный город России, в котором работает клиент «Смарт-Софт». География внедрений решений «Смарт-Софт» включает все регионы России: от Анадыря на востоке до Калининграда на западе и от Певека на севере до Дербента на юге.

SMART-SOFT

ПАМЯТКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМНОМУ АДМИНИСТРАТОРУ

Используйте антивирусы на уровне шлюза

Главный источник вирусов и прочего вредоносного кода — интернет. Установив антивирус на уровне шлюза, вы защитите сразу все компьютеры локальной сети, так как он проверяет проходящий через прокси-сервер трафик. Не забудьте прописать каждому пользователю в качестве прокси-сервера шлюз с антивирусом.

Госкомпаниям необходимо использовать решения, сертифицированные ФСТЭК, например антивирус «Лаборатории Касперского». Помимо него в Traffic Inspector Next Generation можно использовать бесплатный плагин ClamAV, а также подключить другой антивирус, поддерживающий протокол ICAP.

Используйте систему обнаружения/предотвращения вторжений (IDS/IPS)

Атаки на компьютерные сети организаций происходят в основном извне. Целью хакеров может стать как внешний ресурс (например, веб-сайт), так и внутренний (скажем, база данных). Решение — система обнаружения/предотвращения атак (IDS/IPS), которая распознает источники атак и атакуемые машины по определенным сигнатурам сетевого трафика и «очищает» трафик от подобных негативных воздействий. Кроме того, система оповещает администратора о происходящем и создает отчеты действий для того, чтобы по ним можно было провести расследование вторжений.

Как правило, функция IDS/IPS входит в состав универсальных UTM-систем информационной безопасности, причем не только дорогих западных, но и более доступных отечественных (читайте тест: http://blog.smart-soft.ru/2018/09/19/testirovanie_sistemi_obnarujeniya_vt/).

Используйте прокси-сервер для фильтрации сетевого трафика

Часто системному администратору ставят задачу заблокировать нерегламентированные действия пользователей рабочих станций (просмотры видеороликов, общение в соцсетях, скачивание «пиратского» контента). Эти действия не только отнимают рабочее время, но и могут привести к заражению рабочей станции. Для предотвращения подобных действий на прокси-сервере необходимо установить правила блокировки доступа к определенным веб-ресурсам.

Полную версию инструкции читайте: http://blog.smart-soft.ru/2019/03/25/pamyatka/

SMART-SOFT

ПАМЯТКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РУКОВОДИТЕЛЮ

Не пренебрегайте официальными документами

Вышестоящие организации выпускают положения по обеспечению информационной безопасности, регламенты и т. п. Как правило, это малопонятные тексты, написанные канцелярским языком. Попросите системного администратора выделить из них суть и обсудите с ним реализацию главных поставленных задач.

Следите за тем, чтобы сотрудники надежно хранили пароли

Доведите до персонала опасность раскрытия их паролей. Бумажка с шифром, приклеенная к монитору, даст хакеру ключ для взлома всей сети. Поставьте сотрудникам в обязанность менять пароли не реже чем раз в полгода (для наиболее важных сотрудников — раз в квартал).

Распорядитесь о резервном копировании

Резервное копирование — это периодическая запись всех цифровых данных организации на внешний накопитель информации. В случае утраты рабочих данных их можно будет вернуть с помощью бэкапа. Как часто делать бэкапы и как долго их хранить? Оптимальный вариант — часто сохранять недавнюю информацию и долго хранить отдельные срезы, например делать бэкапы каждый день, хранить последние 30 дней, а также хранить срезы, сделанные 2, 3, 6, 12 и 24 месяца назад.

Обучайте персонал информационной безопасности

Базовые вещи объяснит системный администратор, но желательно подходить к вопросу обучения комплексно, используя специальные курсы (например, Kaspersky ASAP). Для новых сотрудников сделать прохождение курсов обязательным.

Проводите периодические проверки

Например, поставьте задачу системному администратору сымитировать хакерскую атаку: отправить всем сотрудникам почтовое сообщение с подменой отправителя и «вирусным» файлом в архиве. Проведите разъяснительную работу среди тех, кто открыл опасное вложение.

КОНТАКТЫ

тел.: +7 (495) 775-59-91, 8 (800) 511-05-81
e-mail: info@smart-soft.ru
www.smart-soft.ru

© 2003-2019, ООО «Смарт-Софт», www.smart-soft.ru