На рынке СМИ
с 1992 года

Groteck
Business Media

ВЕСТНИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МАШИНОСТРОЕНИЕ, МЕТАЛЛУРГИЯ, НЕФТЕГАЗОВЫЙ КОМПЛЕКС, ЭНЕРГЕТИКА, ТРАНСПОРТ, ЖКХ, ТЕЛЕКОММУНИКАЦИИ, БЕЗОПАСНОСТЬ, СТРОИТЕЛЬСТВО, ПИЩЕВАЯ ИНДУСТРИЯ, МЕДИЦИНА, ФИНАНСВЫЙ СЕКТОР, ОБРАЗОВАНИЕ И НАУКА, ИНДУСТРИЯ СЕРВИСА, ТОРГОВЛЯ, СЕЛЬСКОЕ ХОЗЯЙСТВО

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННОЕ АГЕНТСТВО МОНИТОР

iCENTER.ru

№ 10 (127) октябрь 2014

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ЗАКОНОДАТЕЛЬСТВО ЗАКОНОПРОЕКТЫ ТЕХНИЧЕСКОЕ РЕГУЛИРОВАНИЕ ФИНАНСЫ ИНВЕСТИЦИИ ФОНДОВЫЙ РЫНОК БАНКРОТСТВО СЕРТИФИКАЦИЯ ЛИЦЕНЗИРОВАНИЕ СТАНДАРТЫ АУДИТ КАЧЕСТВО СОГЛАШЕНИЯ ПАРТНЕРСТВО СЛИЯНИЯ ПОГЛОЩЕНИЯ РЕОРГАНИЗАЦИИ КАДРОВЫЕ НАЗНАЧЕНИЯ КАДРОВЫЕ РЕШЕНИЯ УПРАВЛЕНИЕ ПЕРСОНАЛОМ ПРОБЛЕМЫ КОНФЛИКТЫ ИНЦИДЕНТЫ АРБИТРАЖНАЯ ПРАКТИКА ПРОЕКТЫ КОМПЛЕКСНЫЕ РЕШЕНИЯ ОПЫТ ВНЕДРЕНИЯ ТЕХНОЛОГИИ ОБОРУДОВАНИЕ ИНСТРУМЕНТЫ МАТЕРИАЛЫ ПРОДУКТЫ УСЛУГИ ОБЗОРЫ ИНДИКАТОРЫ РАЗВИТИЯ АНАЛИТИКА ЭКСПЕРТНЫЕ ОЦЕНКИ ДЕЛОВОЙ КАЛЕНДАРЬ ВЫСТАВКИ ФОРУМЫ КОНФРЕНЦИИ ОБУЧЕНИЕ ПОВЫШЕНИЕ КВАЛИФИКАЦИИ СЕМИНАРЫ ТРЕНИНГИ УЧЕБНЫЕ КУРСЫ ПРОФЕССИОНАЛЬНАЯ ЛИТЕРАТУРА ИСТОРИЧЕСКИЙ КАЛЕНДАРЬ ФАКТЫ

УВАЖАЕМЫЕ КОЛЛЕГИ!

В агентстве "Монитор" открыта непрерывная подписка на издания.

Вы можете оформить подписку с любого месяца по редакционным ценам, которые значительно ниже цен, предлагаемых подписными агентствами.

Для корпоративных подписчиков действуют специальные скидки от 15%.

Звоните: +7 (495) 647-0442 доб. 22-82 или пишите: monitor@groteck.ru

Будем рады видеть вас среди наших читателей!

ВЫБОР РЕДАКЦИИ

СОДЕРЖАНИЕ:

АНОНСЫ

Новинки профессиональной литературы

Обучение / повышение квалификации

Деловой календарь

ИСТОРИЧЕСКИЙ РАКУРС: ОКТЯБРЬ

СПРАВОЧНЫЕ РАЗДЕЛЫ

ЦИТАТЫ НОМЕРА

ВИНСЕНТ УИФЕР
Первый вице-президент, McAfee Labs

Мы должны дать достойный отпор нашим противникам на поле информационной безопасности за счет более тесного сотрудничества и взаимодействия между отраслевыми игроками. Как представители отрасли, мы должны понимать и быть готовы отразить самые сложные комплексные атаки, известные на сегодня и потенциально возникающие завтра...

ЭДУАРД ОСТРОВСКИЙ
Вице-президент, МФИ Софт

По уровню ИТ-услуг Россия не уступает другим развитым государствам. Однако надо отметить как негативный фактор большую зависимость отрасли от поставок зарубежного оборудования и системно-технических решений. В сегодняшней политической обстановке остро встает вопрос информационной безопасности ИТ-систем, что вызывает необходимость импортозамещения...

ГРЭМ КЛУЛИ
Эксперт по информационной безопасности, Eset

Давным-давно, когда о ЦПД можно было только мечтать, айтишники использовали любую возможность уменьшить объем файла. Тогда появился формат ZIP, но у него были и конкуренты. Один из них — ARJ — получился весьма удачным и был незаслуженно забыт впоследствии. Представьте себе мое удивление, когда я обнаружил, что ARJ еще пользуются, пусть даже это мошенники.

БЕН ЛОРИ
Сооснователь, Apache Software Foundation

Инструменты противодействия контроля за действиями в интернете уже существуют, и хотя технически они функционируют отлично, они не всегда отвечают ожиданиям простых пользователей. Многие программы требуют дополнительных усилий при установке или просто выдают непонятные окна, которые вводят пользователей в заблуждение...

ЦИФРЫ. ПРОГНОЗЫ НОМЕРА

процентов мобильных приложений не удовлетворяют базовым требованиям корпоративной безопасности, сообщила исследовательская компания Gartner.

руководителей и специалистов по ИТ и ИБ из 40 субъектов РФ приняли участие в конференции «Информационная безопасность. Региональные аспекты. ИнфоБЕРЕГ-2014».

уникальных IP-адресов зараженных устройств насчитывалось в бот-сети, созданной злоумышленниками с использованием Mac.BackDoor.iWorm, по состоянию на 26 сентября 2014 г.

продуктов компании Symantec заменило одно решение Norton Security. Отказ от разветвленной линейки произошел в интересах пользователей, которые затруднялись с выбором защиты ИБ.

млн атак было осуществлено на российский сегмент интернета за шесть месяцев 2014 г., что связано с сочинской Олимпиадой, а также событиями вокруг Крыма и на юго-востоке Украины.

дня максимально требуется на то, чтобы развернуть облачную услугу информационной безопасности Security-as-a-Service от «Крок» на основе сертифицированных средств защиты информации.

ПРОГНОЗ НОМЕРА: Международная антивирусная компания Eset (Словакия) и фонд «Сколково»

млн рублей от фонда «Сколково» получит победитель конкурса стартапов в области информационной безопасности iSecurity. Его участники получат менторскую поддержку и специальные призы.

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ

Отменено обязательное обезличивание персональных данных, обрабатываемых в информационных системах

18 сентября 2014, Россия, Москва
Источник: news.softodrom.ru

6 сентября 2014 года издано постановление Правительства Российской Федерации № 911, которым внесены изменения в постановление Правительства Российской Федерации от 21.03.2012 № 211. Документом отменяется обязанность операторов персональных данных – государственных и муниципальных органов осуществлять обезличивание персональных данных, обрабатываемых в информационных системах.

Постановление Правительства Российской Федерации было опубликовано на официальном интернет-портале правовой информации pravo.gov.ru 10 сентября 2014 г. и вступает в силу с 18 сентября 2014 г.

Напомним, что в соответствии с постановлением Правительства № 211 оператор персональных данных, являющийся государственным или муниципальным органом, был обязан обезличить персональные данные во всех случаях их обработки в информационных системах.

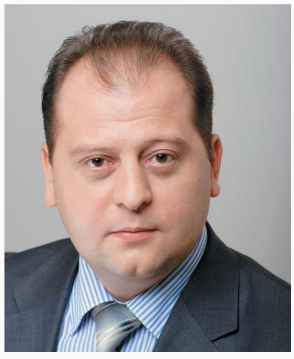
Практика правоприменения продемонстрировала, что обработка персональных данных в государственных и муниципальных информационных системах не всегда требует обезличивания информации. Необходимость применения указанной меры защиты возникает в исключительных случаях, которые установлены российским законодательством. К таким случаям относится необходимость органов государственной власти и местного самоуправления размещать в открытом доступе документы, содержащие персональные данные, например, обезличенные копии судебных актов.

Таким образом, большая часть информационных систем, содержащих персональные данные, не подвержены тем рискам безопасности персональных данных, на нейтрализацию которых направлен институт обезличивания. Однако существовавшая нормативно-правовая база обязывала осуществлять обезличивание персональных данных во всех информационных системах вне зависимости от уровня угроз.

В мае 2014 г. Роскомнадзор инициировал совершенствование института обезличивания, результатом которого стало издание постановления Правительства № 911.

ФСБ России в приказе для операторов персональных данных так и не учла мнение участников отрасли

23 сентября 2014, Россия, Москва
Источник: safe.cnews.ru



Сергей Земков, управляющий директор «Лаборатории Касперского» в России , странах Закавказья и Средней Азии

ФСБ выпустило приказ, описывающий набор мер по обеспечению безопасности персональных данных при их обработке с использованием средств криптозащиты. Большая часть его положений осталась неизменной по отношению к тексту проекта, в отношении которого ведомство еще год назад консультировалась с отраслью. Главная проблема, по мнению экспертов, — необходимость применения исключительно сертифицированных средств криптографии.

«Российская газета» опубликовала приказ ФСБ от 10 июля 2014 г., утверждающий состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке с использованием средств криптозащиты — для каждого из четырех существующих уровней защищенности.

Документ вступит в силу 28 сентября текущего года.

Как прокомментировал CNews пространный текст приказа управляющий директор «Лаборатории Касперского» в России, странах Закавказья и Средней Азии Сергей Земков, речь в нем в основном идет об организационных мерах (безопасности помещений, использовании сейфов, ведении журнала учета машинных носителей персданных и пр.), а также о самой необходимости применения шифрования (криптографии).

Проект данного приказа был опубликован ФСБ еще в начале октября 2013 г., и ведомство как на этапе его подготовки, так и в течение двух недель после размещения текста в интернете собирало предложения отрасли. Судя по обсуждениям на тематических форумах годичной давности и по сегодняшним комментариям экспертов, пожелавших выразить своих мнение без указания их имен, главной претензией к документу было то, что в нем устанавливалась необходимость использовать исключительно сертифици-

рованную криптографию. Специалисты по безопасности считают, что для весьма существенного числа сценариев обработки персональных данных таких средств криптографии просто нет.

Андрей Прозоров, ведущий эксперт InfoWatch по информационной безопасности

Как сообщил CNews ведущий эксперт InfoWatch по информационной безопасности Андрей Прозоров, его компания также направляла в ФСБ свои замечания по поводу проекта приказа. Помимо вышеупомянутых подходов и требований к использованию сертифицированных средств шифрования InfoWatch предлагала пересмотреть и требования по физической безопасности. В сумме эти меры могли бы решить вопрос сложности исполнения требований ФСБ операторами персональных данных. Кроме того компания предлагала пересмотреть саму структуру документа. «К сожалению, замечания были практически не учтены в финальной версии приказа», — говорит Прозоров.

В принятом документе, кроме уже описанных узких мест, операторам, как считает Прозоров, также следует особое внимание уделить положениям приказа, касающимся использования электронных журналов (безопасности и сообщений).

С тем, что очень многие первоначальные требования ФСБ остались в неизменном виде, соглашается и Сергей Земков. «К сожалению, выполнение части из них достаточно нетривиальный процесс, и не очень понятно, как это поможет защите персональных данных», — говорит он.

Андрей Прозоров уточняет, что защита персональных данных с использование криптографических средств регламентировалась ФСБ России и ранее. «До этого операторы выполняли положения двух документов: "методические рекомендации..." и "типовые требования..." (оба от 2008 г). Однако эти документы устарели и стали требовать пересмотра с момента появления постановления Правительства РФ № 1119. Оно определило новые подходы по защите персональных данных, а регуляторам (ФСТЭК и ФСБ) пришлось совершенствовать свои регламенты, — говорит Прозоров. — Подразделения ФСТЭК справились намного быстрее и разработали приказ № 21 на замену приказу № 58», — заключает он.

В Совете безопасности РФ обсудили защиту российского Интернета

02 октября 2014, Россия, Москва
Источник: securitylab.ru

Владимир Путин, президент РФ

Президент РФ Владимир Путин провел заседание Совета безопасности РФ, посвященное противодействию угрозам национальной безопасности в информационной сфере. Об этом сообщается на сайте главы государства.

"Сегодня это одно из приоритетных направлений обеспечения национальной безопасности. Надежная работа информационных ресурсов, систем управления и связи имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для защиты суверенитета России в самом широком смысле этого слова", – заявил Путин.

Президент РФ подчеркнул, что сейчас отдельные страны пытаются использовать доминирующее положение в информационном пространстве для достижения экономических и военно-политических целей. Кроме того, в Интернете распространяются экстремистские и террористические материалы.

По словам Путина, "соответствующие ведомства" регулярно фиксируют атаки на российские информационные ресурсы (какие именно, он не уточнил). "Должен сказать, что за последнее время, за полгода, количество атак увеличилось в разы, просто несопоставимо даже с прошлым годом", – добавил он.

Глава государства констатировал, что необходимо повысить защищенность отечественных сетей связи и информационных ресурсов, обеспечить устойчивость российского сегмента Интернета, а также развивать отечественные информационные технологии. При этом он отметил: "Мы не намерены ограничивать доступ в сеть, ставить ее под тотальный контроль, огосударствливать интернет, ограничивать законные интересы и возможности людей, общественных организаций, бизнеса в информационной сфере".

Напомним, в июле текущего года Минкомсвязь, ФСБ и Минобороны России провели учения по защите российского сегмента Интернета. Также тема защиты инфопространства обсуждалась на июльском саммите БРИКС. В апреле на конференции по вопросу управления инфраструктурой Интернета NETmundial-2014 в Сан-Паулу (Бразилия) министр связи и массовых коммуникаций РФ Игорь Никифоров предложил стремиться к равноправному управлению Интернетом с участием всех стран мира. Сейчас контролем доменных имен, IP-адресов и иных интернет-механизмов занимается международная некоммерческая организация Internet Corporation for Assigned Names and Numbers (ICAAN), созданная при участии правительства США. Заявление Никифорова не было включено в итоговые материалы конференции, что возмутило Минкомсвязи России (оно объявило об этом на своем сайте).

Минкомсвязь России предложило запретить госорганам использовать Google Docs с 1 января 2016 года

02 октября 2014, Россия, Москва
Источник: lenta.ru

Эмблема Минкомсвязи России

Минкомсвязи предложило органам государственной власти с 1 января 2016 года пользоваться облачными услугами хранения и обработки документов, предоставляющимися только российскими компаниями, вычислительная инфраструктура которых находится на территории Российской Федерации. Об этом говорится в проекте федерального закона, подготовленного министерством, с которым ознакомилась «Лента.ру».

Законопроектом предлагается внести изменения в федеральный закон «Об информации, информационных технологиях и о защите информации».

В случае принятия данного закона, госорганы не смогут хранить и редактировать документы в таких популярных облачных сервисах зарубежных компаний, как Google Docs от Google, OneDrive от Microsoft, iCloud Drive от Apple и других.

Кроме того, юрлицам — поставщикам облачных вычислений — необходимо будет получить государственную аккредитацию для оказания услуг.

В проекте сказано, что государственная аккредитация поставщиков услуг облачных вычислений должна производиться федеральным органом исполнительной власти, который «осуществляет функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий». Таким органом на сегодня является Минкомсвязи.

НОВОСТИ ОТРАСЛИ

Финансы. Инвестиции. Фондовый рынок

Kaseya купила Scorpion Software для разработки комплексного решения по управлению идентификацией и доступом к данным

10 сентября 2014, Швейцария
Источник: pcnews.ru

Компания Kaseya, поставщик программных решений по управления ИТ в «облаке», объявила о приобретении Scorpion Software, поставщика решений по безопасности и аутентификации с интегрированными технологиями двухфакторной проверки подлинности и решений по управлению паролями. Об этом CNews сообщили в Kaseya.

Сегодня организации сталкиваются с постоянно растущим набором проблем, связанных с обеспечением доступа к информации. Они должны обеспечить своим сотрудникам безопасный и легкий доступ к растущему числу приложений с любого устройства в любом месте и одновременно эффективно управлять этими задачами, отметили в Kaseya. В то же время, кражи или угрозы встречаются все чаще в нашем мобильном мире. Таким образом, компаниям требуется решение, легкое в управлении и способное обеспечить безопасный доступ к данным.

С объединением своих технологий и AuthAnvil от Scorpion Software компания Kaseya рассчитывает предложить клиентам комплексное решение для управления ИТ, которое обеспечит соблюдение корпоративных политик безопасности.

Так, по информации Kaseya, решение AuthAnvil включает следующие ключевые функции: SingleSignOn (SSO); Web-Based SSO; безопасный удаленный доступ к бизнес-ресурсам практически из любой точки мира; многофакторную аутентификацию; управление учетными данными; обеспечение соответствия требованиям стандартов; Password Automation; аудит паролей.

Acronis купил ведущего американского разработчика «бэкапов в облаках»

18 сентября 2014, США
Источник: biz.cnews.ru

Сергей Белоусов, Гендиректор Acronis

Acronis приобрел американского разработчика решения для восстановления данных в облаке nScaled. Теперь пользователи продуктов Acronis получат возможность быстро возобновлять работу своих систем даже в случае отказа оборудования.

Acronis, разработчик систем восстановления данных, сообщил о приобретении американской компаии nScaled, выпускающая продукт «аварийного восстановления данных как услуга» (Disaster-Recovery-as-a-Service, DRaaS). Сумма сделки не разглашается.

Компания nScaled была основана в 2009 г. в Сан-Франциско, обслуживает несколько сотен клиентов в Северной Америке и Великобритании. Компания поддерживает глобальную сеть облачных центров обработки данных, расположенных в Далласе, Ашберне и Лондоне. По оценке Forester Research, компания является ведущим поставщиком в сегменте DRaaS.

В результате покупки nScaled, ее офис в Сан-Франциско станет представительством Acronis.

Интересно, что одним из инвесторов nScaled является российский венчурный фонд Almaz Capital. В феврале 2012 г. он участвовал в раунде инвестирования в nScaled вместе с инвестиционной компанией Doughty Hanson Technology Ventures и бизнес-ангелами Силиконовой долины. Сумма раунда тогда составила $7 млн.

Almaz Capital Александра Галицкого близок гендиректору Acronis Сергею Белоусову: в частности, Галицким и Белоусовым в 2010 г. был основан инвестиционный фонд Runa Capital.

nScaled предлагает полнофункциональное решение для виртуализации и защиты данных как в локальных, так и удаленных средах. Оно позволяет переключаться на резервные мощности и работать в облаке, а также быстро восстанавливать работу серверов, обеспечивая непрерывность бизнеса. Продукт nScaled поддерживает функции централизованного мониторинга и анализа, с помощью которых можно проверять готовность системы к аварийному восстановлению.

У Acronis уже есть решение для резервного хранения данных в интернете - Acronis Hosted Backup-as-a-Service. Покупка nScaled позволяет компании Acronis создать полный ассортимент услуг облачного резервного копирования и восстановления, включив в него решение по аварийному восстановлению в облаке. Таким образом, пользователи данного сервиса в случае сбоев смогут быстро возобновлять работу, даже если запасное оборудование недоступно, отмечает гендиректор Acronis Сергей Белоусов.

В свою очередь, для nScaled сделка поможет значительно расширить географию своей деятельности, получив доступ к широкой партнерской сети Acronis. Кроме того, разработчики nScaled смогут воспользоваться дополнительными преимущества от использования технологии Acronis AnyData Engine, позволяющей клиентам собирать, хранить, восстанавливать и контролировать данные, а также получать доступ к любым данным в любых средах и на любых устройствах.

«В составе команды Acronis у нас будет доступ к большому количеству ресурсов и мы вольемся в международный коллектив, который поможет нам в развитии услуг по аварийному восстановлению и защите ИТ-инфраструктуры, приложений и данных наших клиентов», - заявил гендиректор nScaled Брэдли Колб (Bradley Kolb).

Глава «Сбербанк капитала» Ашот Хачатурянц и миллиардер Константин Николаев приобрели малоизвестного интегратора «Технопром»

02 октября 2014, Россия, Москва
Источник: forbes.ru

Ашот Хачатурянц, Глава «Сбербанк капитала»

Как ожидается, компания объявит о начале крупного проекта в области информационной безопасности в партнерстве с одним из крупнейших мировых ИТ-вендоров.

Московский интегратор «Технопром» заявил о смене своего собственника.

Согласно распространенному компанией сообщению, новыми хозяевами интегратора стали Ашот Хачатурянц (глава «Сбербанк капитала», «дочки» Сбербанка) и Константин Николаев (совладелец крупного транспортного холдинга «Н-Транс», до 2008 г. носившего имя «Северстальтранс» и частично принадлежавшего владельцу «Северстали» Алексею Мордашову).

Помимо прочего Константин Николаев известен также как соучредитель Московской школы управления «Сколково» и как покупатель в 2006 г.

миноритарного пакета акций компании «Мостотрест», подрядчика дорожного строительства вокруг Сколково.

Начиная с 2011 г. Константин Николаев присутствует в первой сотне рейтинга Forbes «Богатейшие бизнесмены России», где в 2014 г. он занял 87 позицию с результатом $1,2 млрд.

Константин Николаев, предприниматель

Возглавляет «Технопром» с июня 2014 г. Константин Юнов, работавший прежде в крупных телекоммуникационных компаниях (ЮТК, «Мобиком-Кавказ»), и в 2008 г. ставший директором по информационным технологиям ОАО «Мегафон». В 2012 г. в рамках происходивших в операторе кадровых перестановок он покинул «Мегафон» и, по собственным словам, «занимался собственными проектами, в частности, аудитом для крупных корпораций и преподавательской деятельностью».

Помимо имен новых владельцев никакие иные параметры покупки, включая прежнего бенефициара компании и сумму сделки, не раскрываются. «Технопром» не раскрывает и своих операционных данных, рассказывая лишь о своих филиалах в Новосибирске и Таганроге.

Данных о работе интегратора в открытых источниках нет. Собеседники CNews, знакомые с состоянием рынка, подтвердили изданию, что «Технопром» в роли субподрядчика участвовал в ряде проектов, осуществлявшихся в 2013 г. - 2014 г. в интересах федеральных органов власти и известных ФГУП. В рамках этих проектов, по данным CNews, «Технопром» выступал поставщиком оборудования и разработчиком ПО для оказания госуслуг.

Вероятнее всего, сделка по приобретению «Технопрома» Ашотом Хачатурянцем и Константином Николаевым была обусловлена стартом крупного проекта с участием этого интегратора. Ожидается, что в ближайшие дни «Технопром» объявит о начале работ, связанных с развертыванием в России производства ИТ-решений, в том числе в сфере информационной безопасности. Партнером «Технопрома» в проекте выступит один из крупнейших мировых ИТ-вендоров.

Рынок информационной безопасности стагнирует, но спрос на российские аппаратные решения растет

02 октября 2014, Россия, Москва
Источник: osp.ru

Отечественные поставщики аппаратных решений для обеспечения информационной безопасности в 2013 упрочили свои позиции.

Аналитическая компания IDC подготовила отчет о состоянии российского рынка аппаратных решений для обеспечения информационной безопасности за 2013.

По заверению IDC, в прошлом календарном году на российском рынке аппаратных решений ИБ наметились признаки стагнации: совокупный объем продаж сократился на 10,5%, составив чуть менее $221 млн. Как уточнил CNews представитель IDC Russia Сергей Логинов, в 2012 г. объем рынка составлял чуть менее $247 млн.

Основными потребителями оборудования для обеспечения безопасности были компании финансового и телекоммуникационных секторов, вынужденные оперативно реагировать на изменения нормативно-правовой базы, а также государственные структуры, участвующие в реализации крупных инфраструктурных и межведомственных проектов по информатизации.

В IDC утверждают, что т. н. «синдром Сноудена» (Эдвард Сноуден — экс-сотрудник американских спецслужб, в 2013—2014 гг. раскрывший сведения о слежке США за интернет-пользователями и правительствами ряда стран) стимулировал спрос на отечественные решения и технологии ИБ как более предпочтительные для построения критически важных информационных систем госорганизаций и частных компаний.

Как результат, отечественные производители аппаратных решений ИБ продемонстрировали впечатляющие темпы роста на фоне заметного сокращения продаж у ведущих западных поставщиков.

<<...В IDC предполагают, что негативные экономические тенденции в текущем году будут усиливаться, и на рынке аппаратных решений ИБ продолжится спад...>>

В пятерку крупнейших игроков на рынке аппаратных решений безопасности по результатам 2013 г. попали Cisco (24,7% от общего объема рынка), «Алладин Р.Д.» (13,6%), Check Point (12,4%), «Инфотекс» (11%) и «Код безопасности» (9,4%).

По словам Сергея Логинова, годом ранее топ-5 выглядел следующим образом: Cisco — 23,9% рынка, «Аладдин Р.Д.» — 13,6%, Check Point — 10,6%, «Код безопасности» — 7,1%, Stonesoft — 6%.

При простом сопоставлении численных показателей может возникнуть ощущение, что аналитики IDC ошибаются в своих выводах. По итогам двух лет мы видим, что процентные доли рынка у зарубежных компаний Cisco и Check Point увеличились, а отечественный «Аладдин Р.Д.» остался с той же долей.

Однако, как поясняет Логинов, в условиях стагнации рост рыночной доли отдельной компании может означать, что ее продажи в денежном эквиваленте падают медленнее рынка. По его словам, Check Point удалось показать небольшой рост за счет успешной реорганизации российского представительства. Все остальные западные вендоры в 2013 г. продемонстрировали спад в продажах, в том числе Cisco, продажи которой в 2013 г. составили $54,48 млн против $59,11 млн в 2012.

«Единственный российский вендор, у которого был небольшой спад — «Аладдин Р.Д.», — говорит Логинов. — В то же время у «Инфотекса» был двузначный рост. У «Кода безопасности» также стабильный рост ($17 млн в 2012 г и $20,8 млн в 2013 г.)».

Главными аппаратными решениями «Алладин Р. Д.» являются USB-токены и смарт-карты на базе технологии JavaCard с российской криптографией «на борту», поддержкой биометрии и платежных приложений. В портфеле «Инфотекса» — программно-аппаратные средства организации виртуальных частных сетей (VPN) и инфраструктуры открытых ключей (PKI), а также комплексы (или самостоятельные сетевые устройства) обнаружения компьютерных атак ViPNet IDS. «Код безопасности» продвигает на рынке свои комплексы криптографии и аппаратно-программное средство защиты компьютера от несанкционированного доступа.

Как можно было заключить из общения с аналитиком IDC по рынкам информационной безопасности и автором отчета Сергеем Яковлевым, не последнюю роль в успехах «Инфотекса» и «Кода безопасности» сыграл тот факт, что они обновили модельный ряд, развив функциональность и повысив конкурентоспособность своих решений.

В IDC предполагают, что негативные экономические тенденции в текущем году будут усиливаться, и на рынке аппаратных решений ИБ продолжится спад. Однако появление новых законов и отраслевых стандартов, повышение количества и качества угроз, а также появление конкурентоспособных отечественных решений будут способствовать постепенному восстановлению и росту спроса в долгосрочной перспективе.

Сертификация. Лицензирование. Стандарты. Аудит

Система двухфакторной аутентификации Swivel Secure сертифицирована ФСТЭК России

04 сентября 2014, Россия, Москва
Источник: Пресс-релиз

Компания Swivel Secure Ltd. (российское представительство ООО «Свивэл Секьюрити») и эксклюзивный дистрибьютор продуктов компании на территории России и стран СНГ NGS Distribution сообщают о получении сертификата соответствия ФСТЭК (№ 3216) на систему обеспечения двухфакторной аутентификации пользователей «Платформа аутентификации SWIVEL», действительный до августа 2017 года. Сертификат удостоверяет, что платформа аутентификации Swivel является программным средством защиты информации от несанкционированного доступа (НСД) к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции идентификации и аутентификации субъектов доступа, по 4 уровню контроля.

Сертификат выдан на основании результатов сертификационных испытаний, проведённых испытательной лабораторией ОАО «Безопасность информационных технологий и компонентов», и экспертного заключения органа по сертификации ОАО «Научно-производственное объединение «Эшелон».

Полученный сертификат соответствия позволяет применять решение Swivel Secure для аутентификации пользователей в рамках всего спектра проектов информационной безопасности, кроме проектов по защите государственной тайны.

Платформа строгой аутентификации Swivel, включающая в себя запатентованную технологию PINsafe, де-факто является технологическим стандартом бестокенной аутентификации. Платформа Swivel объединяет широчайший спектр современных средств аутентификации – включая решения для таких сегментов, как облачные системы, веб, VPN и VDI. Swivel поддерживает двухфакторную аутентификацию (как бестокенную, так и с физическими токенами) с помощью SMS, мобильного приложения, токенов OATH или телефона, а также средства строгой аутентификации, основанные на показе изображений в браузере.

На сегодняшний день решение Swivel Secure уже применяется в нескольких организациях на территории РФ – в том числе в компании-поставщике трубной продукции и в одном из старейших в России банков Москвы. Проекты по внедрению Swivel Secure ведутся в нескольких компаниях различных сфер бизнеса и обсуждаются с крупнейшими предприятиями РФ.

Авторизованным дистрибьютором решений Swivel Secure на территории России и СНГ является группа компаний NGS Distribution.

Линейка USB-токенов и смарт-карт JaCarta совместима с системой «Интернет-Клиент-Банк» от «Инист»

11 сентября 2014, Россия, Москва
Источник: itsec.ru

Компания «Аладдин Р.Д.», российский разработчик и поставщик решений для обеспечения информационной безопасности, и компания «Инист», специализирующаяся на разработке, внедрении и сопровождении банковских приложений и многопользовательских универсальных биржевых и торговых комплексов, завершили тестовые испытания на совместимость своих продуктов.

Как сообщили CNews в «Аладдин Р.Д.», сертификат совместимости, подписанный компаниями, подтверждает корректность работы смарт-карт и USB-токенов JaCarta в составе программного комплекса «Интернет-Клиент-Банк», который в настоящее время используется более чем в 60 российских банках, в том числе в «Росбанке», «Нордеа Банке», коммерческом банке «ДельтаКредит» и пр.

Согласно результатам тестовых испытаний, для аутентификации, безопасной работы с усиленной квалифицированной электронной подписью и хранения ключей и цифровых сертификатов в системе «Интернет-Клиент-Банк» могут применяться смарт-карты и USB-токены JaCarta ГОСТ и JaCarta PKI/ГОСТ, а также электронные ключи JaCarta ГОСТ/Flash и JaCarta PKI/ГОСТ/Flash.

«Стэп Лоджик» присоединилась к программе ассоциированных консультантов BSI ACP

16 сентября 2014, Россия, Москва
Источник: anews.com

Компания «Стэп Лоджик» выполнила требования «Британского Института Стандартов» (BSI) для вступления в программу ассоциированных консультантов (ACP), подтвердив квалификацию и опыт своих специалистов в разработке и внедрении систем менеджмента информационной безопасности.

Как сообщили CNews в «Стэп Лоджик», программа BSI ACP предназначена для информационной поддержки при выборе компании-консультанта, способной оказать квалифицированную помощь на пути внедрения различных международных стандартов менеджмента. Вступление «Стэп Лоджик» в ACP подтверждает компетенции специалистов компании в области реализации требований международного стандарта ISO/IEC 27001 и выполнения сопутствующих работ.

Стандарт ISO/IEC 27001 определяет универсальный и целостный подход к созданию в организации комплексной системы менеджмента информационной безопасности. Требования стандарта гармонизированы с другими стандартами международной организации по стандартизации (ISO), такими как ISO 9001, ISO 14001, ISO 20000. Кроме того, система менеджмента информационной безопасности, построенная по стандарту ISO/IEC 27001, позволяет в рамках единых процессов обеспечить как защиту ценной для компании информации, так и выполнение актуальных нормативных требований законодательства и регулирующих органов, подчеркнули в компании.

Заложенные в стандарт принципы позволяют успешно применять его в организациях различного масштаба и специфики деятельности. Завершением успешного внедрения стандарта может быть сертификация созданной системы менеджмента информационной безопасности в международной системе сертификации.

«Стэп Лоджик» готова предложить организациям, заботящимся о повышении уровня защищенности информационных активов и эффективном управлении деятельностью по защите информации, полный комплекс консалтинговых услуг в области систем менеджмента информационной безопасности: создание системы менеджмента информационной безопасности в соответствии с требованиями стандарта ISO/IEC 27001; подготовка к сертификации системы менеджмента информационной безопасности по требованиям ISO/IEC 27001; внедрение комплексных систем автоматизации менеджмента информационной безопасности Governance, Risk and Compliance (GRC); внедрение организационных и технических мер защиты информации; аудит и оценка рисков информационной безопасности.

IBS получила сертификат ФСТЭК на систему Parallels VDI

17 сентября 2014, Россия, Москва
Источник: ict-online.ru

Группа компаний IBS, российский поставщик программного обеспечения и ИТ-услуг, получила сертификат ФСТЭК России на систему виртуализации рабочих мест Parallels VDI. Государственный сертификат позволяет использовать решение для обработки сведений конфиденциального характера и применять его в государственных информационных системах, сообщили CNews в IBS.

Продукт Parallels VDI представляет собой защищенное решение для российского рынка, предназначенное для виртуализации рабочих мест (VDI) и позволяющее крупным и средним организациям строить пользовательскую рабочую среду. Полученный сертификат ФСТЭК России № 3218 удостоверяет, что «программный комплекс Parallels VDI 1.0», разработанный компанией Parallels и производимый компанией «ИБС Экспертиза» в соответствии с техническими условиями БКМД.50 1100 1.396-01 30 01, является программным средством со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, реализующим в среде виртуализации функции управления доступом, резервного копирования, контроля целостности и регистрации событий безопасности, соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) — по 4 уровню контроля и технических условий (при выполнении условий по эксплуатации, приведенных в формуляре).

Таким образом, Parallels VDI полностью соответствует российским требованиям к защите информации. Продукт обладает встроенными механизмами безопасности и сертифицирован как серийное изделие, в том числе и по заданному уровню отсутствия недекларированных возможностей (НДВ). Сертификация на отсутствие недекларированных возможностей является обязательной, в том числе, для использования ПО в государственных организациях, компаниях, обрабатывающих большие объемы персональных данных, на предприятиях ВПК, в организациях силового блока и других. Для проведения сертификации программный код продукта был полностью раскрыт для российской испытательной лаборатории, рассказали в IBS.

Сертифицированный продукт Parallels VDI может использоваться при построении ИТ-инфраструктуры, в которой осуществляется обработка сведений конфиденциального характера, персональных данных. Встроенные в продукт механизмы разграничения доступа на базе политик позволяют заказчикам строить ИТ-инфраструктуру с несколькими изолированными контурами безопасности и использовать его в государственных информационных системах 1 и 2 классов защищенности, а также для обеспечения 1, 2 уровней защищенности.

Как отмечается, решение легко интегрируется с подсистемами, входящими в типовую ИТ-инфраструктуру современной организации, такими как централизованный каталог Active Directory, система мониторинга событий информационной безопасности, средства многофакторной идентификации пользователей с использованием цифровых сертификатов и др. Решение позволяет использовать в качестве клиентской платформы как классические десктопы, так и «тонкие» терминалы.

Продукт оптимизирован для работы с различными типами прикладных систем (в том числе ресурсоемких ERP, АБС, «тяжелых» КИС и т.д.), обеспечивает возможность интеграции с различными классами периферийных устройств (принтеры, сканеры, электронные ключи, флэш-устройства и др.).

В качестве основных применений продукта в компании выделяют следующие: построение однородной защищенной пользовательской среды для организации, имеющей среднее или большое количество рабочих мест; построение многоконтурной ИТ-инфраструктуры с различными политиками безопасности; обеспечение безопасной работы мобильных (удаленных) пользователей с корпоративными приложениями. Продукт найдет свое применение в организациях банковской сферы, государственных организациях, госкомпаниях, крупных коммерческих компаниях, в ритейле, в страховом бизнесе и многих других.

КОМПЕТЕНТНОЕ МНЕНИЕ:
Дмитрий Романченко, IBS, директор отделения информационной безопасности

<<Данный продукт — отличный пример совместного комплексного технического решения, которое обеспечивает конкурентоспособные технические и эксплуатационные характеристики, соответствие требованиям по защите информации должного уровня. Данный продукт является одним из блока собственных (совместных) разработок защищенных решений компании IBS, нацеленных на российский рынок.>>

Решение в области информационной безопасности HP TippingPoint получило сертификат соответствия требованиям ФСТЭК России

22 сентября 2014, США
Источник: astera.ru

HP сообщает о том, что решение в области обеспечения кибернетической безопасности HP TippingPoint получило сертификат соответствия «Требованиям к системам обнаружения вторжений» (ФСТЭК России 2011) и «Профилю защиты систем обнаружения вторжений уровня сети четвертого класса защиты» (ФСТЭК России 2012).

Полученный сертификат по HP TippingPoint и SMS №3232 от 12.09.14г (НДВ-4, СОВ-4, 1Г, ИСПДн-1) удостоверяет, что решение является системой обнаружения вторжений со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, и соответствует требованиям руководящих документов: «Защита от несанкционированного доступа к информации. Часть I. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999г.) — по 4 уровню контроля. Требованиям к системам обнаружения вторжений, утвержденным приказом ФСТЭК России от 6 декабря 2011г. № 638 – по 4 классу защиты и может использоваться при создании автоматизированных систем до класса защищенности 1Г включительно в соответствии с требованиями руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992г.), а также для защиты информации в ИСПДн до 1 уровня включительно.

HP TippingPoint – это передовое решение по сетевой безопасности. В связи с повышением сложности угроз, популярности персональных мобильных устройств, появления новых требований к соответствию, популяризации облачных вычислений и повсеместному использованию развлекательных приложений, специалисты по безопасности должны управлять большим количеством рисков. Решения по сетевой безопасности HP TippingPoint обеспечивают гибкую и модульную защиту для приложений, сетей и данных от современных распространенных атак.

Основные функции:

- Защита физических, виртуальных и облачных сетей, а также трафика между приложениями;

- Комплексная защита от угроз при помощи данных от передовых исследований HP DVLabs, проводимых международной группой экспертов;

- Доступ на основе политик.

HP TippingPoint Next Generation Intrusion Prevention System (NGIPS) Представляет новый функционал для безопасности уровня приложений в комбинации с обеспечением осведомленности пользователей и возможностями исследования содержимого входящего/исходящего трафика, продукт NGIPS динамически защищает приложения, сеть и данные от новых и усовершенствованных угроз.

Контроль содержимого обеспечивает предотвращение распространения вредоносного ПО путем изучения входящих и исходящих коммуникаций на предмет контента и исполняемого кода. Это предоставляет возможность для идентификации и блокировки вредоносного трафика, который может осуществлять связь с серверами управления и контроля, а также пытаться украсть пользовательскую информацию.

КОМПЕТЕНТНОЕ МНЕНИЕ:
Андрей Кутуков, HP Software, директор в России

<<В этом году HP отмечает 75-летие компании и одновременно 45-летие присутствия в России. Мы всегда уделяли и будем уделять большое внимание российскому рынку, и сертификация продуктов – еще одно тому подтверждение. Система обнаружения вторжений HP TippingPoint широко известна среди российских специалистов по информационной безопасности, и зарекомендовала себя как надежное, функциональное и удобное в эксплуатации решение. Мы рады, что с прохождением сертификации область применения HP TippingPoint существенно расширилась, и теперь еще большее количество компаний сможет обеспечивать защищенность данных с помощью решений мирового уровня.>>

СУИБ «Технический центр Интернет» сертифицирована на соответствие ISO/IEC 27001

23 сентября 2014, Россия, Москва
Источник: Пресс-релиз

АМТ-ГРУП объявляет об успешной сертификации системы управления информационной безопасностью (СУИБ) компании «Технический центр Интернет» (ТЦИ) на соответствие требованиям стандарта ISO/IEC 27001. Работы по внедрению и подготовке к сертификации СУИБ ТЦИ на соответствие положениям стандарта осуществлялось с привлечением экспертов АМТ-ГРУП. Сертификационный аудит был проведен представительством Британского института стандартов (BSI, British Standards Institute) – международным лидером в области сертификации систем менеджмента.

В область сертификации вошли процессы, непосредственно связанные с основной деятельностью компании: разработка и обслуживание Главного реестра и системы регистрации доменов .RU, .РФ, .SU, .ДЕТИ, .TATAR , .MOSCOW и .МОСКВА, а также обеспечение бесперебойной работы доменной адресации российского сегмента сети Интернет в глобальной сети. ТЦИ является одним из крупнейших специализированных технических центров в Европе, к компании предъявляются высокие требования по информационной безопасности, в том числе со стороны регуляторов ICANN и IANA. Соответствие требованиям ISO/IEC 27001 позволило обеспечить высокий уровень защиты информационных активов ТЦИ.

Работы по приведению СУИБ ТЦИ в соответствие требованиями стандарта ISO/IEC 27001 велись с 2012 года. Основной пласт работ по внедрению стандарта был реализован в начале 2013 года, после чего процессы СУИБ начали функционировать в полном объеме. Спустя год с этого момента прошел первый цикл работы всех процессов СУИБ, и руководством ТЦИ было принято решение начать подготовку к сертификации. Специалистами АМТ-ГРУП был проведен инспекционный аудит, результаты которого позволили говорить о достижении процессами высоких уровней зрелости и готовности ТЦИ к прохождению сертификационного аудита.

Сертификат соответствия получен по версии стандарта ISO/IEC 27001:2005.

Безопасность данных и систем является одним из важнейших аспектов нормального функционирования реестров доменов и всей российской системы доменной регистрации. «Мы несем за это прямую ответственность, – говорит Алексей Платонов, генеральный директор ТЦИ. – Комплексность и сложность систем непрерывно растет, растет количество и разнообразие угроз. В этой ситуации обеспечение ИБ должно восприниматься как «непрерывный процесс», интегрированный в корпоративную модель управления. Для реализации данного процессного подхода мы решили использовать международный стандарт ISO/IEC 27001. Сертификация позволила нам подтвердить достигнутый уровень зрелости процессов ИБ со стороны независимой и авторитетной организации BSI. Для нас это новое подтверждение успешной реализации стратегии ТЦИ в области ИБ».

«С самого начала проекта была поставлена цель в конечном итоге выйти на независимую сертификацию. На протяжении последних двух лет мы наблюдали непрерывное повышение зрелости процессов СУИБ. На текущий момент мы можем говорить о том, что поставленные цели и задачи достигнуты», – отмечает Сергей Терехов, ведущий консультант АМТ-ГРУП, руководивший работами по внедрению стандарта.

«Внедрение СУИБ является сложным процессом, завершение которого сертификацией является нетривиальной задачей. Нам удалось путем проведения аудита ИБ и оказания периодических консультаций для заказчика выявить и устранить проблемные места, которые неизбежно появляются при эксплуатации СУИБ. Тем самым мы минимизировали число возможных несоответствий и выявлений со стороны аудитора BSI», – говорит Александр Пуха, ведущий консультант АМТ-ГРУП, руководивший работами по подготовке к сертификации.

КОМПЕТЕНТНОЕ МНЕНИЕ:
Валерий Темников, ТЦИ, руководитель отдела информационной безопасности

<<Основная часть работ по внедрению стандарта проведена до выхода его новой версии в 2013, поэтому было принято решение сертифицироваться по версии 2005 года. Процесс перехода на новую версию уже идет полным ходом. Сертификация предполагает периодическое проведение инспекционного аудита со стороны BSI для подтверждения соответствия, ближайший аудит запланирован на 2015 год. К этому моменту планируется полностью завершить переход на новую версию.>>

«Аладдин Р.Д.» и «Бифит» протестировали свои продукты на совместимость

30 сентября 2014, Россия, Москва
Источник: uaport.net

Компании «Аладдин Р.Д.», российский разработчик и поставщик решений для обеспечения информационной безопасности, и компания «Бифит», занимающаяся разработкой, внедрением и сопровождением программного обеспечения для электронного банкинга, завершили тестовые испытания на совместимость своих продуктов. Об этом CNews сообщили в «Аладдин Р.Д.».

По результатам тестирования компании подписали сертификат совместимости, который подтверждает корректность работы электронных ключей и смарт-карт JaCarta в составе программного комплекса iBank 2 (начиная с версии 2.0.23.1025).

В частности, в системе электронного банкинга iBank 2 для реализации строгой двухфакторной аутентификации, формирования и проверки усиленной квалифицированной ЭП, а также хранения ключей и цифровых сертификатов могут использоваться USB-ключи и смарт-карты JaCarta ГОСТ и JaCarta PKI/ГОСТ и комбинированные токены с дополнительной Flash-памятью JaCarta ГОСТ/Flash и JaCarta PKI/ГОСТ/Flash.

При этом драйверы для устройств входят в состав современных операционных систем и не требуют установки, подчеркнули в «Аладдин Р.Д.». Работа с токенами и смарт-картами поддерживается в программном комплексе iBank 2 во всех популярных интернет-браузерах, среди которых Microsoft Internet Explorer, Google Chrome, Opera, Safari и Mozilla Firefox.

«РТС-тендер» подтвердила соответствие системы защиты данных требованиям законодательства РФ

02 октября 2014, Россия, Москва
Источник: rts-tender.ru

Компания «РТС-тендер» успешно прошла аттестационные испытания на соответствие положениям и требованиям по защите конфиденциальной информации и персональных данных. Как сообщили CNews в «РТС-тендер», в ходе испытаний было установлено, что информационная система площадки, подсистема обеспечения информационной безопасности и принимаемые меры по защите информации полностью соответствуют требованиям законодательства РФ (а также федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, противодействия техническим разведкам и технической защиты конфиденциальной информации и персональных данных).

Аттестационные испытания площадки включали в себя оценку соответствия системы защиты информации электронной площадки предъявленным требованиям к безопасности конфиденциальной информации и к безопасности при обработке персональных данных. Выполнение данных требований позволило защитить информацию от утечки по техническим каналам, от несанкционированного доступа и от специальных воздействий на нее и ее носители, в том числе DDoS-атак, указали в компании.

Испытания проводились на двух объектах информатизации — центрах обработки данных площадки «РТС-тендер», обеспечивающих требуемую производительность работы системы и сохранность основных информационных массивов. По результатам испытаний площадке «РТС-тендер» были выданы аттестаты соответствия требованиям по защите конфиденциальной информации класса 1Г и персональных данных.

«На площадке "РТС-тендер" уделяется большое внимание информационной безопасности организации, и в настоящее время создана система управления информационной безопасностью в соответствии с международным стандартом ISO/IEC 27001-2013. В рамках этих работ уже построена система защиты конфиденциальной информации по классу 1Г и защищены персональные данные более чем 100 тысяч пользователей, — рассказал генеральный директор «РТС-тендер» Виктор Степанов. — В ближайших планах — международная сертификация и обеспечение непрерывности бизнес-процессов по стандартам ISO 22301».

Новые поступления стандартов в Федеральный информационный фонд технических регламентов и стандартов (выпуск №9-2014)

03 октября 2014, Россия, Москва
Источник: gost.ru

Стандарты ИСО

35 Информационные технологии. Машины конторские

35.240.15 ISO/IEC 7811-2:2014 Карточки идентификационные. Метод записи. Часть 2. Магнитная полоса. Низкая коэрцитивность

35.240.15 ISO/IEC 7816-4:2013/Cor.1:2014 Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 4. Организация, защита и команды для обмена. Техническая поправка 1

35.240.40 ISO/IEC 8484:2014 Информационные технологии. Магнитные полосы на сберегательных книжках

35.100.01 ISO/IEC 9834-8:2014 Информационные технологии. Процедуры для работы регистрационных органов идентификаторов объектов. Часть 8. Создание универсальных уникальных идентификаторов и их использование в идентификаторах объектов

35.110 ISO/IEC 13157-1:2014 Информационные технологии. Телекоммуникации и обмен информацией между системами. Безопасность NFC. Часть 1. Службы и протокол безопасности NFC- SEC NFCIP-1

35.100.10 ISO/IEC 19369:2014 Информационные технологии. Телекоммуникации и обмен информацией между системами. Методы испытания NFCIP-2

35.110 ISO/IEC 24771:2014 Информационные технологии. Телекоммуникации и обмен информацией между системами. Стандарт MAC/PHY на беспроволочную сеть ad hoc для поддержки QoS в производственной рабочей среде

35.240.30 ISO/IEC 26300:2006/Amd.1:2012/Cor.1:2014 Информационные технологии. Формат открытого документа для офисных применений (открытый документ) v1.0. Изменение 1. Формат открытого документа для офисных применений (открытый документ) v1.1. Техническая поправка 1

35.240.30 ISO/IEC 26300:2006/Cor.3:2014 Информационные технологии. Формат открытого документа для офисных применений (открытый документ) v1.0. Техническая поправка 3

35.040 ISO/IEC 29167-1:2014 Информационные технологии. Автоматическая идентификация и методы сбора данных. Часть 1. Службы безопасности для радиоинтерфейсов RFIP.

Соглашения и партнерства. Профессиональные сообщества. Реорганизации

McAfee и Symantec совместно с Fortinet и Palo Alto Networks основали альянс по борьбе с киберугрозами

12 сентября 2014, США
Источник: telegraf.by

Компании Fortinet и Palo Alto Networks сообщили о том, что компании McAfee и Symantec присоединились к альянсу по борьбе к киберугрозами Cyber Threat Alliance в качестве сооснователей.

Как сообщили CNews представители Cyber Threat Alliance, задача альянса — обеспечивать координацию усилий, направленных на борьбу с киберпреступностью, за счет расширенного взаимодействия по вопросам аналитики угроз и обмена индикаторами заражения. Ранее взаимодействие игроков рынка зачастую ограничивалось обменом сигнатур вредоносного ПО. Новый альянс обязует участников предоставлять доступ к расширенным аналитическим сведениям об угрозах, включая информацию об уязвимостях «нулевого дня», данные о серверах командных центров ботнетов, сведения об угрозах для мобильных платформ, indicators of compromise (IoCs), связанных с постоянно совершенствуемыми угрозами (APT), помимо привычного обмена сигнатурами вредоносного ПО. Опираясь на коллективную базу знаний, участники альянса смогут обеспечить более высокий уровень безопасности как конечным пользователям, так и компаниям, считают в Cyber Threat Alliance.

Кроме того, в рамках упорядочения принципов работы альянса и разработки его регламента каждый из сооснователей — Fortinet, McAfee, Palo Alto Networks и Symantec — выделят ресурсы для определения

наиболее эффективных механизмов обмена последними данными об угрозах, что призвано укрепить взаимодействие между участниками альянса.

«Мы должны дать достойный отпор нашим противникам на поле информационной безопасности за счет более тесного сотрудничества и взаимодействия между отраслевыми игроками. Как представители отрасли, мы должны понимать и быть готовы отразить самые сложные комплексные атаки, известные на сегодня и потенциально возникающие завтра. Альянс для обеспечения противодействия угрозам создает необходимую среду для обмена знаниями об инфраструктуре и тактиках, составляющих основу атак», — заявил Винсент Уифер (Vincent Weafer), первый вице-президент McAfee Labs.

«Компания Symantec рада быть учредителем альянса Cyber Threat Alliance, который берет на себя обязательство обеспечивать активный обмен информацией о современных атаках. Работая вместе над созданием решений, способных противодействовать кибератакам следующего поколения, мы добьемся более заметных успехов в борьбе за безопасный интернет для пользователей по всему миру», — считает Адам Бромвич (Adam Bromwich), вице-президент подразделения Security Technology and Response в Symantec.

«Инфотекс» открыла офис в Санкт-Петербурге

22 сентября 2014, Россия, Санкт-Петербург
Источник: infotecs.ru

«Инфотекс», российский разработчик программных и программно-аппаратных VPN-решений и средств криптографической защиты информации, объявила о расширении своего представительства в северо-западном регионе и открытии офиса в Санкт-Петербурге. Появление собственного структурного подразделения в северной столице будет способствовать укреплению взаимоотношений с бизнес-партнерами и заказчиками компании, говорится в сообщении «Инфотекс», поступившем в редакцию CNews.

Ключевой разработкой компании является технология ViPNet, которая предоставляет широкий спектр возможностей построения виртуальных сетей для организаций с большим числом территориально удаленных офисов: от объединения в виртуальную сеть нескольких компьютеров до создания глобальных распределенных виртуальных сетей, работающих в масштабе всей страны. Компания выпускает более 50 различных продуктов на базе данной технологии (программных и программно-аппаратных комплексов), каждый из которых может содержать в себе несколько функциональных модулей.

На сегодняшний день подразделения «Инфотекс», общее число сотрудников которой на данный момент составляет около 500 высококвалифицированных специалистов в области ИБ, уже работают в Москве, Хабаровске. Также есть представители в таких городах, как Уфа, Саратов и Краснодар. Решение об открытии представительства в Санкт-Петербурге обусловлено возрастающим спросом на продукты и решения ViPNet в северо-западном регионе, пояснили в компании. В функции представительства входит: установление и поддержание контактов с государственными органами и деловыми кругами Санкт-Петербурга и Ленинградской области, представление интересов «Инфотекс» на территории региона, укрепление взаимоотношений с имеющимися компаниями-партнерами и поиск новых в целях расширения деятельности компании.

«Наша компания динамично развивается, привлекая клиентов в различных регионах России, — заявил Андрей Чапчаев, генеральный директор «Инфотекс». — Мы ставим перед собой задачу наращивать долю компании на рынке ИБ, предлагая своим заказчикам высокотехнологичные, простые в управлении продукты и решения. Наша компания инвестирует значительные ресурсы в исследования и разработку новых средств ИБ и развитие текущих продуктов. Открытие представительства в Санкт-Петербурге станет очередным шагом в развитии потенциала компании на рынке производства средств защиты информации и развития партнерской сети в регионе».

Zecurion и «Смарт-Софт» разработают совместное решение для защиты данных от утечек

23 сентября 2014, Россия, Москва
Источник: ict-online.ru

Компания Zecurion, разработчик решений для защиты информации от утечек, и ГК «Смарт-Софт», российский разработчик решений для организации и контроля интернет-доступа, объявили о начале стратегического партнёрства. Соглашение о технологическом сотрудничестве подписали исполнительный директор группы компаний «Смарт-Софт» Татьяна Медова и заместитель генерального директора Zecurion Александр Ковалёв, сообщили CNews в Zecurion. В рамках партнёрства технические специалисты компаний разработают совместное комплексное решение на основе продукта Traffic Inspector и систем Zecurion, которое обеспечит комплексный контроль доступа в интернет и полноценную защиту информации от утечек.

Система Traffic Inspector представляет собой сертифицированный интернет-шлюз на базе Windows, способный обеспечивать масштабную антивирусную защиту, контролировать использование интернет-трафика, блокировать баннерную рекламу, фильтровать спам и многое другое. Программа разработана в соответствии с требованиями российского законодательства и полностью отвечает потребностям отечественного ИТ-рынка, отметили в компании.

В свою очередь, в комплекс Zecurion DLP входят системы для решения различных задач в рамках защиты информации: Zgate, Zlock, Zserver и Zdiscovery. Все четыре продукта могут использоваться самостоятельно для решения поставленных перед ними задач, а вместе они составляют комплексную систему, обеспечивающую защиту от утечек информации. Так, Zgate анализирует сообщения, передаваемые по сетевым каналам, Zlock контролирует печать на принтерах и копирование документов на съемные носители, Zserver защищает информацию при хранении на серверах с помощью шифрования, Zdiscovery реализует поиск конфиденциальной информации на компьютерах пользователей и в хранилищах данных.

«Мы рады сообщить, что наш многочисленный партнёрский список пополнился ещё одной российской компанией в сфере разработки решений в области учёта передачи данных, — заявил Александр Ковалёв, заместитель генерального директора Zecurion. — Интеграция с Traffic Inspector позволит Zecurion расширить присутствие на SMB-рынке».

«Сотрудничество с разработчиком DLP-систем даёт нам уверенность в том, что будущие совместные проекты пройдут без видимых трудностей, а также позволит в ближайшее время вывести на рынок востребованный среди заказчиков продукт, — прокомментировала событие Татьяна Медова, исполнительный директор ГК «Смарт-Софт». — На сегодняшний день специалисты обеих сторон ищут совместное техническое решение для систем Zecurion и флагманского продукта нашей компании Traffic Inspector, которое обеспечит не только организацию, контроль и защиту интернет-доступа, но и комплексную защиту данных от утечек».

Google, Dropbox и Open Technology Fund займутся проблемой конфиденциальности в интернете

25 сентября 2014, США
Источник: allnewspoint.com

Google, Dropbox и Open Technology Fund объединились для поддержки организации Simply Secure, которая будет заниматься изучением проблем, возникающих у пользователей при использовании инструментов анонимизации с открытым кодом, и помогать разработчикам с их решением.

Google, Dropbox и Open Technology Fund заявили о поддержке организации Simply Secure, основной целью которой является упрощение доступа пользователей к инструментам анонимизации и средствам обеспечения безопасности. Simply Secure планирует объединить вместе разработчиков ПО, аналитиков и дизайнеров, чтобы выявить проблемы, с которыми сталкиваются пользователи при использовании зашифрованных средств онлайн-коммуникации, и найти решения этих проблем.

Сегодня существует достаточно много решений, направленных на то, чтобы сделать онлайн-коммуникации конфиденциальными и безопасными. Вместо того, чтобы создавать еще больше подобных программ, Simply Secure сфокусируется на поддержке уже имеющихся, их совершенствовании с точки зрения удобства для пользователей путем привлечения дополнительных источников финансирования.

В Экспертный совет организации вошли специалист по защите данных Google и со-основатель Apache Software Foundation Бен Лори (Ben Laurie); разработчик протокола Off-the-Record Messaging (OTR) и профессор Университета Ватерлоо Иан Голдберг (Ian Goldberg); а также Венди Зельцер (Wendy Seltzer), советник по политике World Wide Web Consortium (W3C).

Рост случаев утечек данных и появление все новой информации о контроле за действиями пользователей в интернете в последние несколько лет породили спрос на надежные средства коммуникации. В результате, многие разработчики стали создавать зашифрованные приложения для обмена голосовыми и текстовыми сообщениями и электронные почтовые ящики, средства для анонимизации онлайн-доступа и пр.

"Инструменты противодействия контроля за действиями в интернете уже существуют, и хотя технически они функционируют отлично, они не всегда отвечают ожиданиям простых пользователей, – отметил Бен Лори. - Многие программы требуют дополнительных усилий при установке или просто выдают непонятные окна, которые вводят пользователей в заблуждение. Какой бы гениальной и элегантной ни была технология, никто не будет ей пользоваться, если она не понятна пользователю на интуитивном уровне".

Simply Secure будет заниматься финансированием исследований в области инструментов анонимизации интернет-коммуникаций, а затем работать с дизайнерами и разработчиками над исправлением выявленных проблем. Публичный аудит пользовательских интерфейсов и кода станет ключевой

Eset и фонд «Сколково» договорились о партнерстве

26 сентября 2014, Россия, Москва
Источник: community.sk.ru

Международная антивирусная компания Eset (Словакия) заключила соглашение о партнерстве с фондом «Сколково». Как сообщили CNews с Eset, на первом этапе партнерство предусматривает совместные образовательные инициативы и мероприятия. В частности, Eset станет партнером iSecurity — конкурса стартапов в области информационной безопасности. Его участники получат менторскую поддержку и специальные призы, а победитель — 5 млн рублей от фонда «Сколково».

В состав жюри конкурса войдет Денис Матеев — глава представительства Eset в России и СНГ. Ему предстоит оценивать представленные проекты и выполнять роль ментора участников.

Со своей стороны, фонд «Сколково» поддержит инициативы Eset в области информационной безопасности для малого бизнеса, в первую очередь, конкурс «Eset стартапам», в ходе которого предприниматели обмениваются опытом защиты бизнеса.

«Одна из задач сотрудничества заключается в том, чтобы изменить представление начинающих предпринимателей о безопасности и подчеркнуть ее значимость. Не стоит считать, что защита бизнеса — это решение бесконечных проблем, не нужно тратить на это много времени. Нужно иметь представление о безопасности и работать проактивно. Подчеркнуть роль безопасности и привлечь внимание к данной проблематике мы планируем в рамках проектов "Eset стартапам" и iSecurity», — отметил Денис Матеев.

В рамках сотрудничества Eset и «Сколково» резиденты фонда также получат льготный доступ к корпоративным решениям Eset NOD32 и смогут пользоваться ресурсами вирусной лаборатории компании.

«Сервионика» и «Аладдин Р.Д.» договорились о технологическом партнерстве

26 сентября 2014, Россия, Москва
Источник: novoteka.ru

Компания «Сервионика» (ГК «Ай-Теко»), российский провайдер услуг в области ИТ-аутсорсинга, и компания «Аладдин Р.Д.», российский разработчик и поставщик решений для обеспечения информационной безопасности, заключили соглашение о технологическом партнерстве. Первые совместные разработки компании планируют реализовать в сфере информационной безопасности облачных сервисов и решений для юридически значимого электронного документооборота (ЮЗЭДО), сообщили CNews в «Сервионике».

Продукты «Аладдин Р.Д.» будут предлагаться «Сервионикой» при реализации комплексных проектов в сфере электронного документооборота, а также при предоставлении сервиса «i-Конто» — решения для обмена юридически значимыми электронными документами. Он позволяет оптимизировать не только затраты на подготовку и отправку документов, но и риски, связанные с неполной или неточной отчетностью для контролирующих органов, подчеркнули в компании. Сервис разработан, в первую очередь, для крупных компаний, работающих с большими объемами отчетности, но может быть полезен и компаниям среднего и малого бизнеса. «Сервионика» также предоставляет услугу по интеграции «i-Конто» с уже существующей у клиентов инфраструктурой и бизнес-приложениями.

Обмен документами в сервисе «i-Конто» происходит через телекоммуникационные каналы связи, безопасность которых обеспечивают средства криптографической защиты. «Аладдин Р.Д.» является разработчиком и поставщиком сертифицированных средств защиты, в частности, продуктовой линейки JaCarta, служащей для строгой двухфакторной аутентификации пользователей на веб-порталах, корпоративных ресурсах и в облачных сервисах, электронной подписи, а также безопасного хранения ключей и цифровых сертификатов. Соответствие продуктов «Аладдин Р.Д.» законодательным требованиям (в том числе 63-ФЗ «Об электронной подписи») подтверждено сертификатами ФСТЭК России и ФСБ России.

Для обеспечения безопасного доступа к сервису «i-Конто» и юридической значимости подписываемых электронных документов и производимых операций в сервис встроен кроссплатформенный мультибраузерный плагин JC-WebClient, обеспечивающий взаимодействие веб-приложения с USB-токеном или смарт-картой JaCarta в контексте браузера. Пользователи мобильных устройств также смогут воспользоваться всеми возможностями сервиса с помощью другой разработки «Аладдин Р.Д.» — технологии JC-Mobile, указали в компании.

«Партнерство с компанией "Аладдин Р.Д." расширит возможности "Сервионики" по предоставлению удобных сервисов для ключевых задач наших клиентов. Одна из них — обеспечение прозрачного и оперативного взаимодействия с контрагентами и контролирующими органами. Сервис "i-Конто", дополненный средствами защиты информации от "Аладдин Р.Д.", позволит нашим клиентам организовать юриди-

чески значимый документооборот с минимальными рисками», — заявила Ирина Гришанова, директор по развитию массовых сервисов и продуктов компании «Сервионика».

«Мы расцениваем сотрудничество с компанией "Сервионика" как взаимовыгодный шаг, который позволит объединить функциональные возможности сервиса "i-Конто" и защиту информации, обеспечиваемую решениями компании "Аладдин Р.Д.". Ключевой задачей нашего партнерства является предоставление российским компаниям высокозащищенного сервиса в сфере ЮЗЭДО, полностью соответствующего требованиям регуляторов и обеспечивающего реализацию задач клиентов», — подчеркнула Евгения Царева (Воложенинова), руководитель направления по работе с дистрибьюторами компании «Аладдин Р.Д.».

«НТЦ ИТ Роса» и «Нордавинд» совместно создадут решения для обеспечения общественной безопасности

29 сентября 2014, Россия, Москва
Источник: astera.ru

Российский разработчик защищенных программных решений «НТЦ ИТ Роса» и группа компаний «Нордавинд», разработчик решений в области интеллектуальных систем мониторинга и обеспечения безопасности любого масштаба, подписали соглашение о сотрудничестве в области разработки совместных ИТ-решений. Об этом CNews сообщили в «НТЦ ИТ Роса».

В рамках партнерства компании планируют провести адаптацию продуктов «Нордавинд» под операционные системы «Роса» («Хром», «Никель», «Кобальт»), что позволит создавать отечественные решения для обеспечения общественной безопасности. По словам представителей «НТЦ ИТ Роса», разрабатываемые продукты предназначены, в первую очередь, для удовлетворения потребности в высокотехнологичных программных решениях крупных государственных заказчиков, таких как предприятия военно-промышленного комплекса, а также востребованы другими российскими организациями, в том числе коммерческими.

Как считают в «НТЦ ИТ Роса» и ГК «Нордавинд», данное событие — безусловно, заметный факт не только для самих партнеров, но и для российской ИТ-отрасли в целом, которая в соответствии с требованиями правительства должна достаточно быстро переориентироваться на создание полностью отечественных готовых решений.

«Сервионика» интегрирует свои сервисы с криптографическими средствами «Крипто-Про»

01 октября 2014, Россия, Москва
Источник: cryptopro.ru

Компания «Сервионика» (ГК «Ай-Теко»), российский провайдер ИТ-услуг, и компания «Крипто-Про», разработчик средств криптографической защиты информации и электронной подписи, заключили партнерское соглашение, в рамках которого «Сервионика» получит возможность использовать в своих сервисах всю линейку криптографических средств «КриптоПро». Об этом CNews сообщили в «Сервионике».

Информационная безопасность является одним из важнейших аспектов комплексных проектов «Сервионики» в сфере ИТ-аутсорсинга, услуг датацентров и предоставления облачных сервисов. Это актуально и для услуг компании в сфере юридически значимого документооборота (ЮЗЭДО), где используются механизмы электронной подписи (ЭП), указали в «Сервионике».

В рамках партнерства планируется интеграция сервисов «Сервионики» со всей линейкой криптографических средств, включая продукты «КриптоПро CSP», «КриптоПро JCP», а также «КриптоПро DSS» (при взаимодействии с программно-аппаратным криптографическим модулем «КриптоПро HSM»). В частности, они будут применяться в решении «i-Конто», предназначенном для организации юридически значимого электронного документооборота. Клиенты из среднего и малого бизнеса могут использовать этот сервис как «коробочное» решение, крупным корпоративным заказчикам предлагается дополнительная услуга интеграции ЮЗЭДО в используемые бизнес-приложения. Применение формата оптимизированной подписи в решении «i-Конто» на основе служб меток времени создания подписи (TSP) и актуального статуса сертификата электронной подписи (OCSP) на базе технологий компании «Крипто-Про» поможет доказать юридическую значимость документа в спорных ситуациях и по прошествии длительного периода времени, подчеркнули в компании.

«Реалии жизни и законодательство задают высокую планку для новых решений в отрасли. Интеграция сервиса "i-Конто" с нашими средствами криптографической защиты информации позволит обеспечить критически важный для клиентов уровень информационной безопасности», — заявил Игорь Курепкин, заместитель генерального директора компании «Крипто-Про».

КОМПЕТЕНТНОЕ МНЕНИЕ:
Ирина Гришанова, Сервионика, директор по развитию массовых сервисов и продуктов

<<Роль облачных сервисов в организации бизнес-процессов российских компаний постоянно растет, а требования клиентов к безопасности данных в "облаке" становятся все более сложными. В партнерстве с "Крипто-Про", российским разработчиком средств криптографической защиты информации, "Сервионика" сможет предоставлять клиентам дополнительные возможности для обеспечения безопасной работы с данными в соответствии с актуальными законодательными требованиями и целями заказчиков.>>

HR. Кадровые решения. Персоны

Эдуард Островский вошел в состав руководства «МФИ Софт» в качестве вице-президента

08 сентября 2014, Россия, Москва
Источник: mfisoft.ru


Эдуард Островский, Вице-президентом «МФИ Софт»

Вице-президентом «МФИ Софт» стал Эдуард Островский — генерал-лейтенант, заслуженный работник связи РФ, член Экспертного совета по инновациям Комитета ГД по наукоемким технологиям. Об этом CNews сообщили в компании «МФИ Софт», российском разработчике систем информационной безопасности (системы DLP, защиты от DDoS), систем фильтрации интернет-трафика, систем легального контроля (СОРМ).

По информации компании, многолетний профессиональный опыт Островского включает в себя военную карьеру, государственное управление, реализацию важных специальных проектов, управление оператором связи. В 1954 г. он призван на действительную военную службу в батальон связи дивизии. В армии получил военную специальность Радиотелеграфист 1 класса. Окончил Ульяновское военное училище связи им. Г.К. Орджоникидзе, затем Военную Академию связи им. Маршала Советского Союза С.М. Буденного. С 1954 по 1993 гг. проходил действительную военную службу на различных должностях в подразделениях и частях связи. С 1989 по 1992 гг. являлся заместителем начальника связи Вооруженных сил СССР, с 1992 по 1993 гг. — начальником связи — заместителем начальника штаба Объединённых Вооруженных сил СНГ.

Как крупный специалист в области связи был приглашен на работу в Правительство РФ. так, с 1993 г. Эдуард Островский работал заместителем Министра связи РФ. С 1995 по 2002 гг., будучи заместителем Министра связи РФ, занимался восстановлением и организацией связи в чеченской республике. Более 10 лет являлся заместителем генерального директора компании «Мегафон» по реализации специальных программ и взаимодействию с государственными органами.

«Мой выбор продолжить работу в компании "МФИ Софт" связан с желанием принять участие в развитии ИТ в части ее инновационной сферы, — пояснил Эдуард Островский. — Российские ИТ и отрасль в целом за последнее десятилетие переживает бурный рост. По уровню ИТ-услуг Россия не уступает другим развитым государствам. Однако надо отметить как негативный фактор большую зависимость отрасли от поставок зарубежного оборудования и системно-технических решений. В сегодняшней политической обстановке остро встает вопрос информационной безопасности ИТ-систем, что вызывает необходимость импортозамещения зарубежного оборудования и программного обеспечения. Компания "МФИ Софт" — российская компания-разработчик программно-аппаратных комплексов по информационной защите ИТ-систем от внутренних и внешних угроз безопасности. Разработки компании внедрены в большинстве крупных телекоммуникационных компаний ("Ростелеком", "Мегафон", МТС, "Билайн", "ТрансТелеКом" и др.). Квалификация коллектива (в том числе более 200 штатных программистов) и опыт их работы позволяет компании играть существенную роль в реализации программы импортозамещения зарубежных программно-аппаратных комплексов на российских ИТ-сетях».

В Минкомсвязи России назначен директор департамента международного сотрудничества

17 сентября 2014, Россия, Москва
Источник: lenta.ru

Мария Казанская, Минкомсвязь России

Мария Казанская назначена на должность директора департамента международного сотрудничества Минкомсвязи. Об этом говорится в сообщении министерства.

Она была временно переведена на эту должность в августе 2014 года.

Мария Казанская родилась в Москве в 1982 году. Окончила Московский технический университет связи и информатики по специальности «сети связи и системы коммутации».

В 2010 году Казанская прошла курсы повышения квалификации в Российской академии государственной службы при президенте России по программе «связь с общественностью (PR) в органах государственной власти», в 2012 году — курсы повышения квалификации в Дипломатической академии МИД России по теме «внешняя политика России».

С 1999 по 2008 год работала в различных коммерческих организациях в сфере оказания услуг связи, реализации высокотехнологичного оборудования и программного обеспечения (ПО), в том числе на руководящих должностях.

С апреля 2008 года Мария Казанская работает в Минкомсвязи.

Экс-замглавы Минкомсвязи России Денис Свердлов возглавил СД «Росэлектроники»

01 октября 2014, Россия, Москва
Источник: lenta.ru

Денис Свердлов, председатель совета директоров ОАО «Росэлектроника»

Бывший заместитель главы Минкомсвязи Денис Свердлов был избран председателем совета директоров ОАО «Росэлектроника» (входит в госкорпорацию «Ростех»). Об этом говорится в сообщении компании.

На этом посту он сменил начальника департамента корпоративных процедур и имущественного комплекса «Ростеха» Владимира Литвина.

В новый состав совета директоров, кроме Свердлова, вошли заместитель начальника корпоративно-правового департамента «Ростеха» Жанна Скорина, начальник финансово-экономического департамента «Ростеха» Кирилл Гайдаш, генеральный директор компании «РТ-Информ» Камиль Газизов, начальник департамента корпоративных процедур и имущественного комплекса «Ростеха» Владимир Литвин, генеральный директор «Росэлектроники» Андрей Зверев и директор департамента радиоэлектронной промышленности Минпромторга России Сергей Хохлов.

Денис Свердлов родился в 1978 году в Санкт-Петербурге. В 1995-2000 годы учился в Санкт-Петербургском государственном инженерно-экономическом университете по специальности "Бухгалтерский учет и аудит". В 1995 году работал системным администратором завода "Метиз", в 1997 году — консультантом по внедрению ERP-систем компании МКД (Санкт-Петербург).

В 2000 году Свердлов организовал собственную компанию по внедрению ERP-систем IT Vison. В 2003-м, после слияния компаний IT Vision и "Корус Консалтинг", стал управляющим партнером объединенной компании.

С 2007 по 2012 год возглавлял компанию Yota («Скартел»). В июле 2012 года был назначен заместителем министра связи и массовых коммуникаций Российской Федерации, курировал вопросы в области связи и интернета.

В 2013 году Свердлов покинул пост замглавы Минкомсвязи, оставшись советником. Это было связано со вступлением в силу закона, запрещающего российским чиновникам, их супругам и несовершеннолетним детям владеть зарубежными счетами и активами. На тот момент жена Свердлова имела зарубежный счет, а семья проживала в Европе.

В том же году он покинул министерство по собственному желанию.

Проблемы. Конфликты. Инциденты. IT-угрозы

Новый троян-вымогатель устанавливает пароль на Android-устройства

11 сентября 2014, Россия, Москва
Источник: techsnew.ru

Компания «Доктор Веб» обнаружила очередной троян-вымогатель, обладающий, по сравнению с другими вредоносными программами данного класса, более широким функционалом. Так, помимо блокировки зараженного устройства с типичным требованием выкупа, он также может самостоятельно установить пароль на разблокировку экрана, задействовав для этого стандартную системную функцию, сообщили CNews в «Доктор Веб».

Новый троян, добавленный в вирусную базу Dr.Web под именем Android.Locker.38.origin, является представителем растущего семейства вредоносных программ, блокирующих мобильные устройства пользователей и требующих выкуп за их разблокировку. Данный Android-вымогатель распространяется киберпреступниками под видом системного обновления и после своего запуска запрашивает доступ к функциям администратора устройства. Далее троян имитирует процесс установки обновления, удаляет свой значок с главного экрана, после чего передает на удаленный сервер информацию об успешном заражении и ждет дальнейших указаний.

Команда на блокировку целевого устройства может быть отдана злоумышленниками как при помощи JSON-запроса с веб-сервера, так и в виде SMS-сообщения, содержащего директиву set_lock. Как и многие трояны семейства Android.Locker, Android.Locker.38.origin блокирует устройство, демонстрируя сообщение с требованием выкупа, которое практически невозможно закрыть.

Однако если пострадавший пользователь все же попытается удалить вымогателя, отозвав у вредоносной программы права администратора, Android.Locker.38.origin задействует дополнительный уровень блокировки, отличающий его от прочих подобных Android-угроз, указали в «Доктор Веб». Вначале троян переводит зараженное устройство в ждущий режим, блокируя экран стандартной системной функцией. После его разблокировки он демонстрирует ложное предупреждение об удалении всей хранящейся в памяти устройства информации.

После подтверждения выбранного действия экран устройства снова блокируется, и троян активирует встроенную в операционную систему функцию защиты паролем при выходе из ждущего режима. Вне зависимости от того, была задействована эта функция ранее или нет, вредоносная программа устанавливает на разблокировку мобильного устройства собственный пароль, состоящий из числовой комбинации «12345». Таким образом, зараженный Android-смартфон или планшет окончательно блокируется до получения злоумышленниками оплаты (блокировка может быть снята ими при помощи управляющей команды set_unlock) или выполнения пользователем полного сброса параметров устройства.

Помимо блокировки мобильных устройств, Android.Locker.38.origin также может выступать и в роли SMS-бота, выполняя по команде киберпреступников отправку различных SMS-сообщений, что может привести к дополнительным финансовым потерям.

По информации «Доктор Веб», пользователи «Антивируса Dr.Web для Android» защищены от действий данного трояна.

Эксперты международной антивирусной компании Eset (Словакия) обнаружили новые образцы спам-рассылки, содержащей троян Win32/Injector.BLWX

19 сентября 2014, Словакия
Источник: windowsmax.net

Наибольшее число заражений приходится на Украину и Великобританию, сообщили CNews в Eset.

Антивирусные продукты Eset NOD32 детектируют новую модификацию трояна как Win32/Injector.BLWX. Вредоносное ПО распространяется в приложении к письмам под видом финансовых документов. Троян содержится в файловом архиве, упакованном раритетным архиватором ARJ, который был первоначально разработан для DOS и ранних версий Windows.

«Давным-давно, когда о широкополосном интернете можно было только мечтать, айтишники использовали любую возможность уменьшить объем файла. Тогда появился формат ZIP, но у него были и конкуренты. Один из них — ARJ — получился весьма удачным и был незаслуженно забыт впоследствии. Пред-

ставьте себе мое удивление, когда я обнаружил, что ARJ еще пользуются, пусть даже это мошенники», — заявил Грэм Клули, эксперт по информационной безопасности и блоггер Eset.

По информации Eset, трояны семейства Win32/Injector обладают обширным функционалом. Различные модификации данного ПО используются для скрытой установки других вредоносных программ, кражи персональных данных жертвы, объединения зараженных устройств в ботнет, рассылающий спам или участвующий в DDoS-атаках.

В Linux и Unix найдена масштабная многолетняя «дыра»

25 сентября 2014, США
Источник: roem.ru

Специалист по безопасности обнаружил уязвимость в командной оболочке Bash, масштаб которой превышает масштаб обнаруженной в апреле уязвимости Heartbleed в протоколе шифрования OpenSSL.

Новая уязвимость в командной оболочке Bash существует много лет и может привести к более серьезным последствиям по сравнению с уязвимостью Heartbleed, считает эксперт Роберт Грэм (Robert Graham) из консалтинговой компании Errata Security.

Командный интерпретатор Bash используется многими серверными компонентами и программами в операционных системах, основанных на ядре Linux, и в других Unix-подобных ОС. Уязвимость была обнаружена специалистом по информационной безопасности Стефаном Чазеласом (Stephane Chazelas).

В Bash есть переменные окружения, которые можно задавать согласно специальному синтаксису при вызове оболочки. Оболочка запускается и задает значения переменных, прописанные в синтаксисе. Уязвимость заключается в том, что непосредственно в самом задаваемом значении переменной можно дописать произвольные команды, которые оболочка также выполнит. В случае если Bash назначена системной оболочкой по умолчанию, она может быть использована злоумышленниками для проведения сетевых атак на серверы с применением веб-запросов.

Например, в выражении env x='() { :;}; echo vulnerable' bash -c "echo this is a test" видно, что переменной x присваивается значение () { :;}; echo vulnerable, в котором содержится другая команда — вывода на экран текста «vulnerable».

Таким образом, пользователи могут легко проверить, есть ли в их системе уязвимость, просто запустив терминал и введя выражение env x='() { :;}; echo vulnerable' bash -c "echo this is a test". Это также могут сделать пользователи Unix-совместимой операционной системы Apple OS X, которая также содержит интерпретатор Bash.

При действующей в системе уязвимости терминал возвращает сообщения «vulnerable» и «this is a test»; а если баг устранен, то «bash: warning: x: ignoring function definition attempt», «bash: error importing function definition for 'x'» и «this is a test» (ошибка в синтаксисе).

Тест в последней актуальной версии OS X 10.9.5 Mavericks показал, что уязвимость присутствует.

«Серьезность этой уязвимости заключается в том, что командную оболочку Bash использует огромное количество различных программ. По этой причине ситуация аналогична уязвимости Heartbleed в популярном протоколе OpenSSL», — пояснил Роберт Грэм. «При этом, в отличие от Heartbleed, касающейся определенной версии OpenSSL, уязвимость в Bash существует очень долгое время. Это означает, что она присутствует в просто огромном количестве устройств, подключенных к сети. Количество систем, которым необходим патч и для которых этот патч никогда не появится, намного превышает количество систем в случае с Heartbleed», — добавил эксперт.

По аналогии с Heartbleed уязвимости в Bash также было дано кодовое имя — ShellShock.

Уязвимость в протоколе шифрования OpenSSL, получившая название Heartbleed, была обнаружена в апреле 2014 г. специалистами компаний Codenomicon и Google. Она позволяла хакерам получать доступ к содержимому оперативной памяти серверов, в которой могли находиться персональные данные пользователей. Уязвимость стала самой масштабной в истории, так как затрагивала около 500 тыс. вебсайтов по всему миру.

Как пишет Ars Technica, некоторые компании, включая саму Red Hat, уже выпустили патчи, устраняющие ошибку Shellshock. Обновления также доступны для некоторых версий CentOS, Ubuntu и Debian.

Таможенников уличили в сговоре с поставщиком при закупке ПО и услуг поддержки Oracle

26 сентября 2014, Россия, Москва
Источник: tendery.ru

ФАС признала незаконной осуществленную ФТС закупку продуктов для анализа приложений и услуг поддержки СУБД Oracle. Ранее этим же контрактом заинтересовался Следственный комитет.

Федеральная антимонопольная служба (ФАС) установила факт нарушения законодательства со стороны Федеральной таможенной службы (ФТС), которое произошло в ходе проведения в мае 2012 г. открытого аукциона на закупку услуг техподдержки систем управления базами данных (СУБД) Oracle и продуктов для поиска уязвимостей в приложениях, работающих на этой СУБД.

Внимание на эти нарушения обратила Счетная палата, которая и передала соответствующую информацию в ФАС.

Победителем аукциона стала компания «СБЛ-Техноложис», получившая за свои работы 332 млн. руб. Поставляемые ею продукты должны были уметь находить и исправлять различные уязвимости в исходном коде: предоставление неограниченных прав в системе, обход систем авторизации, возможность не исполнять часть кода в тестовой среде и т.д.

Комиссия ФАС установила, что поставку решений для контроля исходного кода и техническую поддержку продуктов Oracle не следовало объединять в единый лот. В результате, по мнению ФАС, были созданы необоснованные преимущества для «СБЛ-Технолоджис». Кроме того, ФАС установила, что данная компания имела приоритетный доступ к тендерной документации, что также предоставило ей необоснованные преимущества.

Контракт с ФТС должен был закончиться в конце 2013 г. В ФАС отмечают, что работы по контракту уже выполнены. В связи с выявленными нарушениями возбуждено административное производство по ст. 18 Закона «О защите конкуренции», посвященной нарушениям при госзакупках.

Виновным должностным лицам ФТС грозит штраф. Кроме того, будет возбуждено отдельное административное производство по ст. 16 того же закона (запрещает согласованные действия органов исполнительной власти и других организаций, если они приводят к повышению цен, ограничению доступа на рынок и т.д.), по которой штраф может быть наложен уже на саму ФТС, причем в размере до половины от стоимости закупки.

Отметим, что в ходе аукциона цена закупки не была снижена. Кроме «СБЛ-Техноложис» заявку подавала еще одна компания, но ее предложение не было допущено к торгам. Согласно данным портала госзакупок, в ходе проведения данного тендера в ФАС направлялись две жалобы.

Компания «Артель» жаловалась, что оператор электронной площадки, на которой проводился аукцион - «Сбербанк - АСТ» - не обеспечил технической возможности компании подать заявку. А компания НВТ жаловалась на условия тендерной документации, в частности, указание требований по аппаратной платформе и недостаточно четкие требования к поставляемому ПО. Первая из этих жалоб была отклонена, о результатах рассмотрения второй жалобы на портале госзакупок не сообщается.

Представитель «СБЛ-Технолоджис» от комментариев отказался. В ФТС к моменту публикации не ответили на запрос CNews.

Принадлежащая Вячеславу Лысакову компания «СБЛ Технолоджис» в 2011-2012 г.г. выиграла целый ряд тендеров ФТС на общую сумму около 700 млн рублей. В 2013-2014 гг., по данным реестра госконтрактов, компания не выигрывала вообще ни в одном тендере.

Известно, что в конце 2013 г. Следственный комитет возбудил уголовное дело о мошенничестве при выполнении госконтракта на поставку ПО для нужд ФТС. По версии следствия, двое столичных бизнесменов с помощью неназванных сотрудников таможенной службы помогли победить в конкурсе компании «СБЛ-Техноложис», из-за чего государство закупило ПО с переплатой около 140 млн.руб.

Обнаружен новый ботнет для Mac OS X

29 сентября 2014, Россия, Москва
Источник: vsesmi.ru

В сентябре 2014 г. вирусные аналитики компании «Доктор Веб» исследовали сразу несколько новых угроз для операционной системы Apple Mac OS X. Одна из них — это сложный многофункциональный бэкдор, добавленный в вирусные базы под именем Mac.BackDoor.iWorm. Как сообщили CNews в «Доктор Веб», данная программа позволяет выполнять на инфицированном «маке» широкий набор различных команд, поступивших от злоумышленников.

При создании данной вредоносной программы злоумышленники использовали языки программирования C++ и Lua, при этом в архитектуре бэкдора широко применяется криптография. В процессе установки троян распаковывается в папку /Library/Application Support/JavaW, после чего дроппер собирает «на лету» файл plist для обеспечения автоматического запуска этой вредоносной программы.

В момент первого запуска Mac.BackDoor.iWorm сохраняет свои конфигурационные данные в отдельном файле и пытается прочитать содержимое папки /Library, чтобы получить список установленных в системе приложений, с которыми бэкдор не будет в дальнейшем взаимодействовать. Если «нежелательные» директории обнаружить не удается, бот получает с использованием нескольких системных функций наименование домашней папки пользователя Mac OS X, от имени которого он был запущен, проверяет наличие в ней своего конфигурационного файла и записывает туда данные, необходимые ему для дальнейшей работы. Затем Mac.BackDoor.iWorm открывает на инфицированном компьютере один из портов и ожидает входящего соединения, отправляет запрос на удаленный интернет-ресурс для получения списка адресов управляющих серверов, после чего подключается к удаленным серверам и ожидает поступления команд для последующего выполнения. Примечательно, что за списком адресов управляющих серверов бот обращается к поисковому сервису сайта reddit.com, указывая в качестве запроса шестнадцатеричные значения первых 8 байт хэш-функции MD5 от текущей даты.

<<...По информации «Доктор Веб», Mac.BackDoor.iWorm способен выполнять два типа команд: различные директивы в зависимости от поступивших бинарных данных или Lua-скрипты...>>

По результатам поиска reddit.com отдает веб-страницу со списком управляющих серверов ботнета и портов, которые злоумышленники публикуют в виде комментариев к теме minecraftserverlists.

Троян пытается установить соединение с командными серверами, перебирая в случайном порядке первые 29 адресов из полученного списка и отправляя запросы на каждый из них. Повторные запросы к сайту reddit для получения нового перечня отправляются раз в 5 минут.

В процессе установки соединения с управляющим сервером, адрес которого выбирается из списка по специальному алгоритму, троян пытается определить, не добавлен ли этот адрес в список исключений, и обменивается с ним специальным набором данных, по которым с использованием ряда сложных математических преобразований проверяется подлинность удаленного узла. Если проверка прошла успешно, бот отправляет на удаленный сервер номер открытого на инфицированном компьютере порта и свой уникальный идентификатор, ожидая в ответ поступления управляющих команд.

По информации «Доктор Веб», Mac.BackDoor.iWorm способен выполнять два типа команд: различные директивы в зависимости от поступивших бинарных данных или Lua-скрипты. Набор базовых команд бэкдора для Lua-скриптов позволяет выполнять следующие операции: получение типа ОС; получение версии бота; получение UID бота; получение значения параметра из конфигурационного файла; установка значения параметра в конфигурационном файле; очистка конфигурационных данных от всех параметров; получение времени работы бота (uptime); отправка GET-запроса; скачивание файла; открытие сокета для входящего соединения с последующим выполнением приходящих команд; выполнение системной команды; выполнение паузы (sleep); добавление нода по IP в список «забаненных» узлов; очистка списка «забаненных» нодов; получение списка нодов; получение IP-адреса нода; получение типа нода; получение порта нода; выполнение вложенного Lua-скрипта.

Собранная специалистами «Доктор Веб» статистика показывает, что в бот-сети, созданной злоумышленниками с использованием Mac.BackDoor.iWorm, по состоянию на 26 сентября 2014 г. насчитывалось более 17 тыс. уникальных IP-адресов зараженных устройств. Наибольшее их количество — 4610 (что составляет 26,1% от общего числа) — приходится на долю США, на втором месте — Канада с показателем 1235 адресов (7%), третье место занимает Великобритания — здесь выявлено 1227 IP-адресов инфицированных компьютеров, что составляет 6,9% от их общего числа.

Троян-вандал для Android форматирует карту памяти и препятствует общению пользователей

30 сентября 2014, Россия, Москва
Источник: udf.by

Компания «Доктор Веб» обнаружила новую вредоносную программу, предназначенную для работы на смартфонах и планшетах под управлением ОС Android. Как сообщили CNews в «Доктор Веб», зловред представляет для пользователей весьма серьезную опасность, поскольку удаляет все имеющиеся на карте памяти данные, не позволяет прочитать входящие SMS-сообщения, а также мешает нормальному общению в популярных программах-мессенджерах, блокируя их окна.

Новый Android-троян, внесенный в вирусную базу «Доктор Веб» под именем Android.Elite.1.origin, является представителем весьма редкого типа вредоносных программ, относящихся к классу программ-вандалов. Такие вредоносные приложения обычно создаются вирусописателями не для получения каких-либо материальных выгод, а для доказательства своих навыков программирования, выражения своей точки зрения

на те или иные события, либо с целью развлечения или хулиганства. Часто подобные угрозы демонстрируют различные сообщения, портят пользовательские файлы и мешают нормальной работе зараженного оборудования. Именно так и действует новый Android-троян, который распространяется под видом популярных приложений, таких, например, как игры, рассказали в компании.

При запуске Android.Elite.1.origin обманным путем пытается получить доступ к функциям администратора мобильного устройства, которые якобы необходимы для завершения корректной установки приложения. В случае успеха троян приступает к немедленному форматированию подключенной SD-карты, удаляя все хранящиеся на ней данные. После этого вредоносная программа ожидает запуска ряда популярных приложений для общения.

Как только пользователь попытается запустить официальный клиент социальной сети Facebook, программу WhatsApp Messenger, Hangouts, либо стандартное системное приложение для работы с SMS-сообщениями, Android.Elite.1.origin блокирует их активное окно, демонстрируя на экране изображение с текстом OBEY or Be HACKED. При этом данная блокировка сохраняется только для указанных программ и не распространяется на прочие приложения или операционную систему в целом, отметили в «Доктор Веб».

Чтобы еще больше ограничить доступ пользователя к инструментам «мобильного» общения, троян препятствует прочтению всех вновь поступающих SMS-сообщений, для чего скрывает от своей жертвы все оповещения о новых SMS. В то же время, сами сообщения сохраняются и заботливо помещаются в раздел «Входящие», который, впрочем, остается недоступным из-за действующей блокировки.

Помимо форматирования SD-карты и частичной блокировки средств коммуникации, Android.Elite.1.origin с периодичностью в 5 секунд рассылает по всем найденным в телефонной книге контактам SMS со следующим текстом: «HEY!!! [имя контакта] Elite has hacked you.Obey or be hacked». Кроме того, похожий текст отправляется в ответ на все входящие SMS, поступившие с действующих мобильных номеров других пользователей: «Elite has hacked you.Obey or be hacked».

Таким образом, счет мобильного телефона большинства пострадавших владельцев зараженных мобильных устройств может быть опустошен за считанные минуты и даже секунды.

Специалисты «Доктор Веб» не рекомендуют пользователям загружать приложения из сомнительных источников. Предоставлять доступ подобным приложениям к правам администратора мобильного устройства также не рекомендуется во избежание порчи файлов или иных негативных последствий.

Злоумышленники используют уязвимость ShellShock

30 сентября 2014, Словакия
Источник: news.21.by

Злоумышленники активно используют уязвимость ShellShock для установки вредоносных программ на Linux-серверы. Об этом CNews сообщили в международной антивирусной компании Eset (Словакия).

Критическая уязвимость ShellShock была обнаружена в конце сентября. Она присутствует во всех версиях командного интерпретатора Bash, который используется в различных дистрибутивах и модификациях Linux, Unix, Apple OS X и Android. С ее помощью злоумышленники могут удаленно устанавливать в уязвимые системы вредоносное ПО. С точки зрения масштаба и возможных последствий ShellShock можно сравнить с известной Heartbleed, ей присвоен наивысший десятый уровень опасности по шкале оценки уязвимостей, указали в компании.

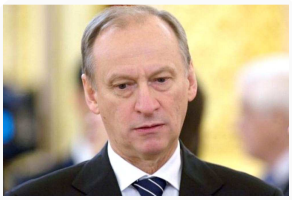
В течение нескольких дней после обнаружения ShellShock специалисты Eset наблюдали несколько вариантов вредоносных программ, которые устанавливались на Linux-серверы с помощью эксплуатации данной уязвимости. Для этого используется специальный HTTP-запрос, который приводит к срабатыванию уязвимости в интерпретаторе Bash. Сам интерпретатор вызывается одним из CGI-скриптов, который получает поля этого HTTP-запроса, сформированного злоумышленником. В качестве текста полей запроса злоумышленники указывают определенную последовательность символов, а затем задают команды для копирования вредоносного файла с удаленного сервера и его исполнения.

Антивирусные продукты Eset NOD32 еще до обнаружения уязвимости ShellShock защищали пользователей от действия этих вредоносных программ, детектируя их как Linux/DDoS.M и OSX/Tsunami.A. Первая представляет собой бэкдор, который используется злоумышленниками для исполнения команд на зараженном сервере. Linux/DDoS.M может выступать и в роли DDoS-бота — получив соответствующие команды, программа будет посылать сетевые пакеты выбранной жертве. В свою очередь, OSX/Tsunami.A — это DDoS-бот, ориентированный на компьютеры под управлением Apple OS X.

Эксперты Eset рекомендуют системным администраторам установить соответствующие обновления для используемых дистрибутивов Linux, а пользователям — сменить пароли для веб-сервисов, так как они могут быть скомпрометированы.

На рунет за 6 месяцев 2014 было осуществлено 57 млн атак

01 октября 2014, Россия, Москва
Источник: lenizdat.ru



Николай Патрушев, секретарь Совбеза РФ

На российский сегмент интернета за шесть месяцев 2014 г. было осуществлено 57 млн атак, что связано с сочинской Олимпиадой, а также событиями вокруг Крыма и на юго-востоке Украины, заявил секретарь Совбеза РФ Николай Патрушев.

Как сообщает «Интерфакс», он отметил, что «активно действуют зарубежные спецслужбы. Мы также фиксируем деятельность экстремистских и террористических групп, а также преступных образований».

Патрушев обратил внимание на то, что работа в России в основном ведется на зарубежном телекоммуникационном оборудовании и программном обеспечении. «Для обеспечения стабильности нашего сегмента интернета нам нужно заниматься тем, чтобы у нас появилось свое телекоммуникационное оборудование, нам нужно обеспечивать свое программное обеспечение. Это делается, но пока недостаточно», - сказал он.

Данная информация была озвучена 1 октября на заседании Совета Безопасности, посвященном "защите информационного пространства России от современных угроз", сообщается на официальном сайте Кремля. Президент России Владимир Путин, который и открыл заседание, отметил, что "нам необходимо выработать и реализовать комплекс дополнительных мер в области информационной безопасности".

Комплекс, по мнению главы государства, подразумевает под собой четыре составляющие. Во-первых, необходимо позаботиться о качественной защите отечественных информационных ресурсов и сетей, чтобы исключить незаконное вмешательство в их работу, а также утечку персональных и иных конфиденциальных данных. Во-вторых, встает вопрос о безопасности самого российского сегмента интернета. Важно обеспечить его бесперебойную работу. Третье направление - это развитие отечественных информационных продуктов, техники и технологий. И, наконец, последнее, на что обратил внимание президент, - это обеспечение международной информационной безопасности. Однако сделать это будет возможным только при расширении сотрудничества как с региональными, так и с глобальными структурами и организациями.

В свою очередь помощник президента Игорь Щеголев по итогам заседания Совбеза России по противодействию угрозам нацбезопасности России в информационной сфере рассказал, что прошедшие в России межведомственные учения по предотвращению попыток нарушить работу рунета показали его уязвимость.

«Вопрос возник ровно потому, что мы сейчас живем в режиме санкций, и, в частности, санкций в банковской сфере. Исходя из такой постановки вопроса западными странами, во многом и была продиктована повестка дня сегодняшнего заседания», - заявил Щеголев.

Главный вопрос, по его словам, заключается в том, «насколько наша страна готова выжить в условиях потенциального применения такого рода санкций и по другим направлениям информационных технологий».

«Страна очень сильно завязана на эти технологии, и общество, и госуправление, и силовые структуры. Наши граждане не мыслят себя без общения через интернет. Проведенные летом учения показали, что страна уязвима. Она, конечно, преодолеет возможные трудности, но есть ряд мер, которые необходимо предпринять», - сказал помощник главы государства.

Логотип и наименование ICANN используются в фишинговых атаках

02 октября 2014, США
Источник: mywebs.su

В последнее время возросло число фишинговых атак, использующих наименование и логотип корпорации ICANN. Об этом в своем блоге сообщил старший инженер ICANN по вопросам безопасности Дейв Пицителло. По его словам, стандартный сценарий атаки выглядит следующим образом: регистрант домена получает якобы от ICANN сообщение электронной почты, уведомляющее об истечении срока регистрации и предлагающее продлить этот срок. Для этого пользователю рекомендуется перейти по содержащейся ссылке и ввести для оплаты продления данные своей банковской карты, говорится в заявлении «Координационного центра национального домена сети Интернет».

Между тем, корпорация ICANN заверяет, что не имеет никакого отношения к подобным сообщениям. ICANN не занимается регистрацией доменных имен и не взимает плату с регистрантов — все это находится в ведении конкретных компаний-регистраторов. Сообщения такого рода являются фальшивками, направленными на похищение финансовой информации пользователей.

Получателям фишинговых сообщений категорически не следует переходить по содержащимся в них ссылкам и тем более сообщать какую-либо информацию. Обо всех подобных случаях рекомендуется сообщать в корпорацию ICANN, ведущую активное расследование этого мошенничеств.

ПРОЕКТЫ. КОМПЛЕКСНЫЕ РЕШЕНИЯ. ОПЫТ ВНЕДРЕНИЯ

Компания «БСС-Безопасность» выполнила работы по защите информации для Администрации Губернатора Московской области

04 сентября 2014, Россия, Московская обл.
Источник: bankir.ru

Компания «БСС-Безопасность», центр компетенции Группы компаний BSS в сфере информационной безопасности, сообщает о завершении проекта по оказанию услуг в области технической защиты информации ограниченного доступа на объектах информатизации Администрации Губернатора Московской области.

В ходе реализации проекта выполнена модернизация объектов информатизации за счет установки и настройки комплекса программно-технических средств защиты информации, сертифицированных ФСТЭК России, проведена периодическая аттестация и ежегодный инструментальный контроль защищенности объектов информатизации.

Компания «БСС-Безопасность» является лицензиатом ФСБ России, ФСТЭК России и Роскомнадзора. Штат компании составляют высококвалифицированные специалисты, обладающие успешным опытом в области разработки, проектирования и внедрения систем технической защиты информации, аттестации объектов информатизации по требованиям безопасности информации, создания, эксплуатации и поддержки защищенных каналов связи, а также в области обеспечения деятельности Удостоверяющих центров.

Компания «БСС-Безопасность», центр компетенции Группы компаний BSS в сфере информационной безопасности, проводит работы по комплексной защите и аттестации объектов информатизации, обследованию информационных систем персональных данных, разработке моделей угроз и нарушителей персональных данных, подготовке к лицензированию заказчиков по направлениям ФСБ России и ФСТЭК России.

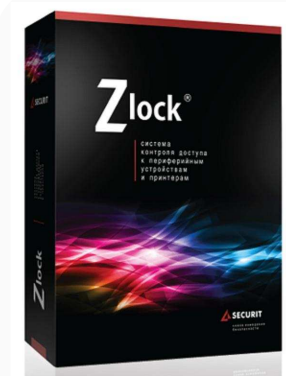
«БСС-Безопасность» аккредитована ФСТЭК России в качестве органа по аттестации объектов информатизации, что расширяет её возможности и позволяет проводить аттестацию объектов информатизации, обрабатывающих сведения, содержащие государственную тайну.

Удостоверяющий центр «БСС-Безопасность» аккредитован Минкомсвязи России на соответствие требованиям Федерального закона от 06.04.2011 г. №63-ФЗ «Об электронной подписи», входит в сети доверенных Удостоверяющих центров ФНС России, ПФР, ФСС РФ, Росстат, Росалкогольрегулирования.

Zecurion обеспечила защиту корпоративных данных ГК «МОРТОН» с помощью DLP-системы Zecurion Zlock (Device Control)

16 сентября 2014, Россия, Москва
Источник: Пресс-релиз

Группа компаний «МОРТОН» — один из ведущих российских застройщиков, входящий в тройку лидеров рынка по объёмам строительства. Совокупный портфель проектов компании превышает 7,5 млн кв. метров жилья, а выручка по итогам 2013 года превысила 51,1 млрд руб. Общая численность сотрудников ГК «МОРТОН» составляет более 5 500 человек.



Zecurion Zlock (Device Control)

В информационной сети ГК «МОРТОН» хранятся и ежедневно используются в работе большие объёмы конфиденциальных данных, утечка которых может привести к серьёзным финансовыми и репутационным потерям. Именно поэтому руководством компании было принято решение о повышении степени защищённости данных. По результатам проведённого анализа рисков, ИБ-специалисты «МОРТОНа» пришли к выводу, что в первую очередь необходимо усилить контроль конечных точек сети. При этом важно было не только обеспечить защиту от утечек через съёмные носители, но и внедрить DLP-систему в сжатые сроки, не нарушив привычный документооборот.

В процессе тестирования ИБ-специалисты «МОРТОНа» провели сравнение DLP-систем Zlock (Device Control) и DeviceLock, по итогам которого остановили свой выбор на решении от компании Zecurion, как наиболее полно отвечающем всем требованиям застройщика. Ключевым отличием Zlock от конкурирующего продукта стал не только быстрый ввод системы в эксплуатацию, но и гибкие настройки политик безопасности для каждого пользователя, а также наличие удобной консоли управления агентами Zlock.

Zecurion Zlock (Device Control) предназначен для защиты от утечек кон-

фиденциальной информации на конечных точках сети. Zlock контролирует все документы и файлы, которые копируются сотрудниками на съёмные устройства и распечатываются на локальных и сетевых принтерах. В отличие от других агентских систем, Zecurion Zlock (Device Control) способен предотвращать утечки информации через устройства в реальном времени. При выявлении нарушений политик безопасности система блокирует печать, чтение или запись конфиденциальных данных на устройства.

Принимая во внимание положительный опыт использования DLP-системы Zecurion, ГК «МОРТОН» планирует увеличить количество лицензий Zlock и Zgate для оснащения DLP-решением большего числа рабочих станций.

КОМПЕТЕНТНОЕ МНЕНИЕ:
Антон Поздняков, МОРТОН, ведущий специалист по информационной безопасности

<<Решающими факторами в пользу DLP-системы Zecurion стали удобная консоль управления агентами Zlock и удобная система отчётности, благодаря которой можно легко проследить кто, как и когда использует съёмные носители. Ещё одной важной для нас функцией стала совместимость с продуктами для проектирования Autodesk, которые ежедневно используют в работе сотни наших сотрудников. Внедрение решения Zlock позволило решить сразу несколько основных задач, стоящих перед нашей командой.>>

«Газпром нефть» первой внедряет отказоустойчивую платформу хранения данных Hitachi VSP G1000 с помощью «Астерос»

25 сентября 2014, Россия, Москва
Источник: softkey.info

Группа «Астерос» и Hitachi Data Systems (HDS), дочернее предприятие Hitachi, Ltd., объявляют о старте проекта в «Газпром нефти», цель которого – увеличение технологической мощности и надежности системы хранения за счет новой платформы Hitachi Virtual Storage Platform G1000. По итогам проекта «Газпром нефть» станет первой компанией в России, которая апробирует на практике новые технологии от Hitachi.

Программа глобальной трансформации ИТ-платформы «Газпром нефти» была инициирована для решения как текущих, так и стратегических задач компании. Одним из её этапов, в частности, был проект по модернизации вычислительных систем «Газпром нефти» и миграции 48 бизнес-приложений SAP. Партнером проекта, реализованного одновременно в двух дата-центрах нефтяной компании в Санкт-Петербурге и Омске, была выбрана компания «Астерос Консалтинг». В фокусе следующего этапа программы трансформации ИТ-инфраструктуры «Газпром нефти» – создание единой среды хранения для всех видов данных с использованием технологий виртуализации. Для этих целей была выбрана мощная отказоустойчивая платформа Hitachi Virtual Storage Platform G1000, анонсированная HDS в апреле текущего года. Партнером проекта вновь стала группа «Астерос».

«Мы предприняли ряд шагов для создания одной из самых высокотехнологичных, отказоустойчивых и надежных ИТ-платформ в нефтяном секторе, – комментирует Константин Кравченко, начальник департамента информационных технологий, автоматизации и телекоммуникаций "Газпром нефти". – Выбор в пользу Hitachi VSP G1000 продиктован стремлением уйти от необходимости внесения коренных изменений в ИТ-системы в ответ на растущие потребности как бизнеса, так и рынка. Внедрение этой платформы поможет нам агрегировать информацию о продажах и сбыте, обеспечить управление производственными базами данных и резервным копированием. В перспективе мы планируем перенос на обновленную платформу дополнительных данных, а также расширение проекта по виртуализации рабочих мест для более чем 10 000 пользователей».

<<...В фокусе следующего этапа программы трансформации ИТ-инфраструктуры «Газпром нефти» – создание единой среды хранения для всех видов данных с использованием технологий виртуализации...>>

Платформа Hitachi VSP G1000 является принципиально новым продуктом японской корпорации, который позволяет реализовать концепцию непрерывно функционирующей облачной инфраструктуры (Continuous Cloud Infrastructure, CCI) в центрах обработки данных нового поколения. Система VSP G1000 отличается высокой адаптируемостью и позволяет планомерно наращивать пропускную способность блочного хранилища до более чем 3 млн операций ввода-вывода в секунду (IOPS), обеспечивая

полезную пропускную способность свыше 48 Гбит/с и производительность NFS более 1,2 млн операций в секунду для унифицированных конфигураций.

«На данный момент VSP G1000 является вершиной в разработке высокопроизводительных надежных инфраструктур и подтверждает лидерство Hitachi Data Systems в этой области, – комментирует Юрий Скачков, Генеральный директор компании Hitachi Data Systems в России и странах СНГ. – Благодаря гибкости и усовершенствованным возможностям, платформа VSP G1000 позволяет быстро адаптировать ИТ-инфраструктуру компании к изменениям потребностей бизнеса без проблем и затрат, связанных с постоянной заменой технологий на более новые. Это новый класс продуктов, рассчитанный на долгосрочное использование и нацеленный на обеспечение максимальных преимуществ для бизнеса компаний. И мы очень рады, что одна из ведущих российских нефтяных компаний – "Газпром нефть" – сможет первой в стране оценить на практике эффективность новейших технологий Hitachi».

Со своей стороны в «Астерос» отмечают: «Наш предыдущий опыт работы с "Газпром нефтью" предполагал перенос на новую аппаратную платформу критичных бизнес-систем, охватывающих практически полный цикл работы нефтяного предприятия, – комментирует Лев Николау, глава "Астерос Консалтинг". – Этот проект сразу задал высокую планку в нашем сотрудничестве, и мы рады, что снова были выбраны в качестве партнера, с которым "Газпром нефть" планирует развивать созданную систему хранения данных и наращивать технологическую мощность своей инфраструктуры. Уверен, что став пионером освоения новых технологий, заложенных в Hitachi VSP G1000, "Газпром нефть" сможет создать необходимую ИТ-платформу для достижения заявленных бизнес-целей».

«Астерос» помог «дочке» «МегаФона» разработать концепцию ИБ

29 сентября 2014, Россия, Москва
Источник: rb.ru

Группа «Астерос» объявила о завершении проекта по разработке концепции развития направления информационной безопасности (ИБ) в «МегаЛабс» (100% дочерней компании оператора «МегаФон»). Реализация данной концепции дает возможность выстроить систему обеспечения ИБ, отвечающую требованиям регуляторов и современным тенденциям в области защиты информации, сообщили CNews в «Астерос».

«МегаЛабс» — российский разработчик продуктов и сервисов в области цифрового контента, медиа, мобильной рекламы, облачных решений, M2M- и геосервисов, IP-коммуникаций. Обладая экспертизой в части разработки инновационных продуктов и монетизации технологий, «МегаЛабс» уделяет значительное внимание вопросам информационной безопасности и защиты интеллектуальной собственности. В рамках стратегического планирования бизнеса в среднесрочной перспективе в компании было решено унифицировать подход к вопросам обеспечения ИБ, сформировать единую политику ИБ и спланировать работы по данному направлению. К выполнению проекта была привлечена команда «Астерос Информационная безопасность».

Первый этап стартовал в октябре 2013 г.: специалистами «Астерос Информационная безопасность» был проведен аудит состояния ИБ в «МегаЛабс». В его контур вошли такие области, как управление кадрами, распределение ролей и обязанностей по ИБ, идентификация и классификация информационных активов, оценка и обработка рисков ИБ, физическая безопасность и защита от воздействий окружающей среды, сетевая безопасность, управление доступом, работа с мобильными устройствами, удаленная работа, антивирусная безопасность, резервное копирование, управление уязвимостями информационных систем, мониторинг и управление инцидентами ИБ, обеспечение ИБ в жизненном цикле информационных систем, взаимодействие с поставщиками и другие.

В рамках обследования был проведен анализ исходных данных, полученных в результате изучения документов по ИБ и серии интервью с ответственными сотрудниками «МегаЛабс», а также оценка степени соответствия систем управления и обеспечения ИБ компании требованиям международных стандартов ISO/IEC 27001-2013 и ISO/IEC 27002-2013. Эксперты «Астерос Информационная безопасность» использовали собственную систему показателей ИБ и методику их оценки. По итогам обследования были определены направления развития информационной безопасности и рекомендации по повышению уровня защиты информационных ресурсов, исходя из степени их критичности для бизнеса.

В рамках следующего этапа для «МегаЛабс» был сформирован план развития направления информационной безопасности на ближайшие 3 года. Финальный этап проекта подразумевал разработку комплекта политик «МегаЛабс», регламентирующих основные направления ИБ. По итогам работ «МегаЛабс» была представлена концептуальная модель комплексной системы обеспечения ИБ, определяющая необходимые процессы, документы и системы обеспечения ИБ, а также план их реализации.

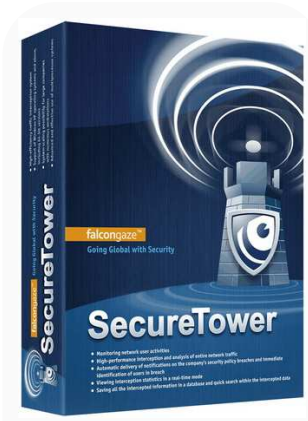
«Специфика бизнеса "МегаЛабс" связана с интеллектуальной составляющей в разработке продуктов и услуг для абонентов "МегаФон" — для нас это был интересный опыт, и мы надеемся продолжить сотрудничество уже на стадии реализации мероприятий по защите информационных ресурсов компании», — заявил Дмитрий Бирюков, руководитель практики аудит и консалтинг «Астерос Информационная безопасность».

КОМПЕТЕНТНОЕ МНЕНИЕ:
Евгений Тулупов, МегаЛабс, руководитель направления ИБ

<<Реализация подготовленной консультантами "Астерос Информационная безопасность" концепции развития информационной безопасности для нас является первым шагом к созданию комплексной системы обеспечения ИБ. В ближайших планах развития данного направления — целый ряд проектов, направленных на совершенствование процессов и систем управления и обеспечения ИБ.>>

СО ЕЭС внедрил SecureTower в семи филиалах

01 октября 2014, Россия, Москва
Источник: stfw.ru



программный комплекс SecureTower

В семи филиалах «Системного оператора Единой энергетической системы» (СО ЕЭС) внедрен программный комплекс SecureTower, предназначенный для контроля каналов утечки данных. Об этом CNews сообщили в компании Falcongaze, разработчике решения.

Организации, представляющие сферу электроэнергетики, склонны следовать требованиям федерального закона N 98-ФЗ от 29 июля 2004 г. «О коммерческой тайне» и принимать соответствующие меры по обеспечению сохранности корпоративной информации, составляющей коммерческую тайну. СО ЕЭС не является исключением и уделяет значительное внимание вопросам защиты от утечки конфиденциальных данных, а также контролю соблюдения организационных мер по обеспечению информационной безопасности. Ранее в рамках реализуемой в компании политики безопасности в исполнительном аппарате СО ЕЭС в Москве был внедрен программный комплекс SecureTower. Теперь продуктом Falcongaze также оснащены семь филиалов организации.

«При выборе инструмента для защиты информации наибольшее внимание мы уделяли функциональным составляющим программных продуктов, которые позволили бы контролировать максимально возможное число каналов утечки и обеспечить тем самым комплексную защиту наших корпоративных данных. После тестирования ряда DLP-систем мы остановили свой выбор на SecureTower от компании Falcongaze. Использование этого программного обеспечения в исполнительном аппарате в течение года принесло ощутимые результаты. Как следствие, в этом году было принято решение о внедрении программного комплекса SecureTower в семи объединенных диспетчерских управлениях СО ЕЭС», — сообщила Анна Васькова, специалист отдела информационной безопасности СО ЕЭС.

«Одной из особенностей корпоративной информационной системы нашей организации является территориальная распределенность. В силу этого нам необходим был инструмент с централизованным управлением, который можно было бы использовать с учетом существующей политики безопасности организации. Продукт компании Falcongaze, как показало время и практика, оказался тем самым инструментом, который в полной мере устроил нас как с функциональной точки зрения, так и с точки зрения удобства использования», — заявил Александр Зализный, ведущий эксперт отдела информационной безопасности СО ЕЭС.

ЛОКО-Банк принял решение о внедрении DeviceLock

01 октября 2014, Россия, Москва
Источник: devicelock.com

Коммерческий банк "ЛОКО-Банк" (ЗАО), занимающий 6 строку рейтинга крупнейших банков России по кредитованию предприятий малого и среднего бизнеса, и уже более 20 лет активно работающий на розничном рынке банковского сектора по всей России, начал эксплуатацию программного комплекса DeviceLock DLP Suite. В ходе поиска решения, обеспечивающего защиту конфиденциальной информации от утечек, специалисты Банка рассматривали различные системы.

Как сообщает начальник Управления поддержки информационно-технологической инфраструктуры КБ "ЛОКО-Банк" Роберт Гасбоевич Гацалов, "Мы пришли к выводу, что оптимальным предложением на рынке, соответствующим потребностям Банка в решении задач защиты информации, является программный комплекс DeviceLock Endpoint DLP Suite. Благодаря внедрению DeviceLock, которое прошло легко и успешно, нам удалось решить одну из важнейших проблем информационной безопасности в Банке".

Информационная сеть «Ригла» под защитой Eset NOD32

02 октября 2014, Россия, Москва
Источник: esetnod32.ru

Международная антивирусная компания Eset объявила о начале сотрудничества с аптечной сетью «Ригла». Для защиты информационной сети был выбран комплексный корпоративный продукт Eset NOD32 Smart Security, говорится в заявлении Eset, поступившем в редакцию CNews.

Аптечная сеть «Ригла» действует в Москве, Санкт-Петербурге, Нижнем Новгороде и других городах России. «В нашей сети — больше 1000 аптек в разных городах России, поэтому важнейшим требованием к антивирусному продукту было удобство централизованного управления, — рассказал Александр Мамлай, начальник отдела информационно технологической инфраструктуры аптечной сети «Ригла». — Сеть расширяет ассортимент и набор услуг, мы храним персональные данные участников дисконтной программы — вся эта информация нуждается в защите. Мы выбрали Eset NOD32 и остались довольны своим решением — при должном уровне защиты от угроз решение требует минимум времени системных администраторов и абсолютно незаметно для обычных пользователей».

Eset NOD32 Smart Security Business Edition — это флагманское корпоративное решение для информационной защиты рабочих станций, файловых серверов и мобильных устройств. Продукт позволяет оперативно распознавать все интернет-угрозы, в том числе неизвестные прежде, за счет сочетания интеллектуальной облачной технологии Eset Live Grid и запатентованного метода эвристического анализа ThreatSense, отметили в компании.

Eset NOD32 Smart Security Business Edition оперативно реагирует на попытки проникновения вредоносных программ, отражает сетевые атаки, детектирует опасные ссылки, а также блокирует нежелательную почту. Оптимизированные алгоритмы сканирования обеспечивают высокую производительность решения, а инструменты управления позволяют оперативно развертывать и администрировать систему антивирусной защиты любого масштаба, утверждают в Eset.

ТЕХНОЛОГИИ. ОБОРУДОВАНИЕ. ПРОДУКТЫ. УСЛУГИ

Oracle представила Key Vault для защиты критически важной служебной информации

09 сентября 2014, США
Источник: oracle.com

Корпорация Oracle представила Oracle Key Vault — программный комплекс класса software appliance, разработанный для безопасного управления ключами шифрования и другой служебной информацией в центре обработки данных предприятия. Как сообщили CNews в Oracle, полностью интегрированный программный комплекс разработан для аппаратной платформы x86-64. Он использует операционную систему Oracle Linux, включенную в дистрибутив для упрощения установки, и СУБД Oracle Database для обеспечения требуемых уровней безопасности, доступности и масштабируемости. Key Vault, оптимизированный для технологического стека Oracle, включая Oracle Database и Oracle Fusion Middleware, может быть с легкостью развернут в существующих средах.

Как отметили в корпорации, надежность шифрования напрямую зависит от безопасности и эффективности процедур управления ключами. Поскольку организации все чаще выполняют шифрование данных как в пассивном автономном режиме, так и в активном онлайн-режиме, безопасное управление всеми ключами шифрования и другой служебной информацией в корпоративном центре обработки данных становится серьезной задачей. Организациям, в то же время, необходимо обеспечивать и соблюдение жестких требований законодательства к безопасному управлению ключами и сертификатами.

Помочь решить эти насущные задачи призван Oracle Key Vault, новейшее дополнение в портфолио средств безопасности Oracle Database. По словам разработчиков, он обеспечивает безопасное централизованное управление ключами шифрования и другой служебной информацией в центре обработки данных, в том числе wallet-файлами Oracle (стандартными зашифрованными файлами, которые безопасно хранят ключи

и связанные метаданные, используемые компонентами технологического стека Oracle), хранилищами Java KeyStores, keytab-файлами Kerberos, файлами ключей SSH и файлами сертификатов SSL.

Среди важнейших функций и возможностей Key Vault в корпорации отметили: быстрое архивирование и восстановление данных — новое решение позволяет архивировать wallet-файлы Oracle, хранилища Java KeyStores и другие файлы учетных данных в главном (master) репозитории, поддерживая легкое восстановление и совместное использование файлов; централизованное управление — реализованная в Oracle Key Vault консоль управления на основе браузера предлагает функции администрирования с интерфейсом point-and-click, упрощенную регистрацию серверов и подготовку аудиторских отчетов; оптимизированные возможности совместного использования файлов — организации могут безопасно использовать wallet-файлы Oracle в кластерах баз данных или средах аварийного восстановления (продукт отлично подходит для работы с Oracle Real Application Clusters, Oracle Active Data Guard и Oracle GoldenGate); гибкость — в средах Oracle Database, использующих опцию Oracle Advanced Security с функциональностью Transparent Data Encryption (TDE), Key Vault управляет TDE-ключами через прямое сетевое соединение — как альтернатива локальному wallet-файлу Oracle; обеспечение соблюдения стандартов — благодаря поддержке протокола KMIP (Key Management Interoperability Protocol), разработанного организацией OASIS, Key Vault может управлять ключами от KMIP-совместимых клиентов.

КОМПЕТЕНТНОЕ МНЕНИЕ:

Випин Самар, Oracle, вице-президент по технологиям безопасности баз данных

<<Поскольку ужесточающиеся регуляционные нормы во всем мире требуют шифрования все более широких категорий конфиденциальных данных, организациям необходимо иметь единое решение для безопасного управления всеми ключами шифрования и другой служебной информацией в своих центрах обработки данных. Oracle Key Vault является основанным на стандартах комплексом, который позволяет организациям сократить издержки, связанные с соблюдением требований законодательства, с помощью решения, которое защищает мастер-ключи шифрования Oracle Database, wallet-файлы Oracle, данные Java KeyStores и другую служебную информацию.>>

«МФИ Софт» анонсировала DLP-систему на основе принципов «Больших данных»

10 сентября 2014, Россия, Москва
Источник: golnet.ru

Компания «МФИ Софт» представила DLP-систему нового поколения — «Гарда Предприятие» 3. Как сообщили CNews в «МФИ Софт», в основе решения лежат принципы Big Data («Больших данных»), многоуровневая аналитика и простой веб-интерфейс.

Как известно, системы DLP — главный инструмент контроля безопасности информационных потоков предприятия. С развитием технологий данных для анализа становится слишком много, и формализовать все правила работы с информацией без ущерба для бизнеса невозможно. Кроме того, обычно такие системы сложны в использовании и требуют большего количества времени специалистов. «МФИ Софт» принципиально изменила взгляд на логику DLP-систем, разработав удобный инструмент для ежедневного использования — «Гарда Предприятие» 3, заявили в компании.

Система хранения данных в «Гарде Предприятие» 3 обеспечивает тотальную запись всех информационных объектов предприятия, передаваемых сотрудниками, и быстрый поиск по накопленной базе. Благодаря применению методики хранения и анализа Big Data в DLP-системе «Гарда Предприятие» появились широкие возможности анализа накопленной информации — автоматическое построение картины информационного обмена, ретроспективный анализ любого инцидента, выявление паттернов и статистических аномалий.

Среди других ключевых возможностей решения «Гарда Предприятие» 3: система отчётности — построена по технологии drill-down, предоставляет многоуровневую аналитику по широкому спектру параметров (связи сотрудников, схемы распространения документов по предприятию, различные статистические графики); интерактивный кроссплатформенный интерфейс — интуитивно понятный даже без чтения инструкции; система хранения данных собственной разработки — позволяет хранить информацию любых объёмов и обеспечивает быстрый доступ к ним (при этом для организации хранилища не требуется дорогостоящего оборудования).

«Мы отошли от традиционного представления о DLP-системе как о сложном специализированном инструменте и пересмотрели поход к хранению и анализу данных. Мы расширили стандартный функционал методами работы с Big Data, — рассказал о новой разработке Владимир Пономарев, заместитель генерального директора «МФИ Софт». — Данный подход позволяет посмотреть на картину коммуникаций в комплексе, построить карту движения информационных потоков и выявить отклонения. Мы предлагаем новый подход к ретроспективному анализу и открываем новые возможности для оценки информационных рисков и угроз еще до того, как они стали инцидентами».

HP расширила портфель услуг и решений для безопасной печати

12 сентября 2014, США
Источник: softp.ru

Компания HP расширила свой ассортимент услуг и решений в области печати. Как сообщили CNews в HP, данные услуги и решения представлены новым брендом компании — HP JetAdvantage, который объединяет широкий спектр решений HP для обработки и печати документов. Так, в рамках HP JetAdvantage корпоративным клиентам предлагается комплекс продуктов для мобильной печати, обеспечения безопасности печати, управления процессами обработки документов и парком устройств печати, которые позволяют оптимизировать основные бизнес-процессы и выполнение отдельных задач с целью снижения затрат и повышения производительности труда.

Среди новых продуктов HP — центр обеспечения безопасности HP Imaging and Printing Security Center 2.1, который позволяет упростить развертывание системы безопасности и мониторинга парка принтеров HP благодаря оптимизации трудоемкого процесса настройки сетевых политик безопасности для устройств печати. Использование центра безопасности HP IPSC позволяет снизить риск несанкционированного доступа в корпоративную сеть и повысить уровень соблюдения стандартов, не увеличивая при этом непроизводительные издержки ИТ, отметили в компании.

HP также предлагает услуги по анализу безопасности печати HP Print Security Advisory Services, которые предусматривают проведение анализа инфраструктуры печати, настройку оптимальной политики безопасности и предоставление рекомендаций по выбору решений для обеспечения безопасности рассматриваемой инфраструктуры. Аналитические услуги HP Print Security Advisory Services будут доступны в странах Европы, Ближнего Востока, Африки и Северной Америки в ноябре 2014 г.

В свою очередь, многофункциональные устройства (МФУ) HP LaserJet Enterprise flow серии M630 имеют более 200 встроенных функций безопасности, инструментарий для обработки документов в соответствии с корпоративными стандартами, а также оснащаются дополнительно приобретаемым модулем криптографической защиты HP (TPM-чипом), который позволяет обеспечить безопасность информационных ресурсов клиентов сразу при подключении устройства.

Арсенал средств безопасности HP также пополнился новыми решениями для мониторинга и проверки инфраструктуры печати и управления ее настройками на всех уровнях: от устройств и обрабатываемых данных до печатаемых документов. Они обеспечивают соблюдение требований информационной безопасности и иных корпоративных стандартов.

Расширены функциональные возможности системы контроля безопасности печати HP ArcSight, которая теперь позволяет вести мониторинг параметров безопасности всех принтеров и МФУ HP, оснащаемых технологией FutureSmart. Собирая, анализируя и сопоставляя информацию о регистрируемых устройством печати событиях, данная система автоматически выводит информацию о рисках на панели HP ArcSight, которая дает полное представление о состоянии безопасности корпоративных ИТ-ресурсов, рассказали в HP.

HP Secure Content Management and Monitoring solution — решение для защиты содержания документов, которые идут в печать — позволяет снизить риск несанкционированного доступа к информации через функции печати, сканирования, копирования и факсимильной связи. Благодаря использованию комплекса средств управления данными HP Autonomy Information Governance данное решение позволяет одновременно вести мониторинг и проверку всей информации, проходящей через МФУ HP, и, таким образом, сразу выявить попытки несанкционированного доступа к документам.

Решение для управления и мониторинга контента HP Secure Content Management and Monitoring Solution будет доступно в странах Европы, Ближнего Востока, Африки и Северной Америки зимой 2014.

КОМПЕТЕНТНОЕ МНЕНИЕ:
Прадип Джотвани, LaserJet, старший вице-президент по технологиям

<<С увеличением финансовых последствий информационных утечек неизбежно растет и потребность в комплексных решениях обеспечения безопасности печати. Компания HP пополняет свой ассортимент, куда входят устройства, решения и услуги под брендом LaserJet, новой системой безопасности HP Print Security Innovations для мониторинга и управления настройками безопасности печати.>>

«Дозор-Джет» — инструмент информационной и экономической безопасности

18 сентября 2014, Россия, Москва
Источник: Пресс-релиз

Компания «Инфосистемы Джет» объявляет о выходе нового релиза программного комплекса «Дозор-Джет» 5.0.4. Ключевая особенность релиза – наличие инцидентной модели расследования. Обновленный управленческий интерфейс системы позволяет интерпретировать и визуализировать необходимые для расследования данные в удобной форме с различным уровнем детализации.

Инцидентная модель превращает DLP-систему в инструмент расследования фактов нарушения информационной и экономической безопасности, повышающий эффективность ИБ- и СБ-служб, позволяя им выявлять и пресекать факты мошенничества или коммерческого сговора сотрудников на начальных стадиях.

Новый функционал позволяет разбирать инциденты на трех уровнях:

- Оперативный уровень: система автоматически ведет мониторинг и анализ всех корпоративных коммуникаций сотрудников, создавая инциденты по событиям ИБ и присваивая им необходимый уровень критичности. На основе этих данных также формируется уровень доверия к каждому сотруднику. Сотрудник ИБ или СБ на этом уровне может перенаправить отдельные инциденты для более глубокой проверки или же пометить инцидент как ошибочный.

- Тактический уровень: аналитик ИБ имеет возможность напрямую из окна инцидента просматривать досье участников коммуникации, выполнять глубокий анализ и расследование инцидента, в том числе на основе выявленных системой внутренних взаимосвязей между участниками подозрительной коммуникации (как внутри компании, так и вовне). Результат работы – расследование и квалификация инцидента ИБ, выявление причастного к нему круга лиц. По итогам расследования формируется отчет для руководства.

- Стратегический уровень предусматривает работу руководителя служб ИБ или СБ и бизнес-руководства по принятию управленческих решений на базе отчетов, создаваемых в системе.

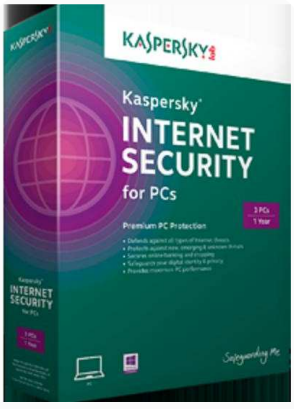
Технологии, используемые в «Дозор-Джет», позволяют при возросшем объеме работ, выполняемых комплексом, сохранить высокую производительность системы фильтрации: поток данных перехватывается и анализируется на скорости до 10 Гбит/с.

«Этот релиз переводит продукт из классических ИБ-систем в класс бизнес-систем, используемых, в том числе, и для обеспечения экономической безопасности. После модуля "Досье сотрудников", увеличения скорости разбора трафика и перехода к хранению данных по технологиям Big Data, реализованных в предыдущих релизах "Дозор-Джет", логичным стало введение инцидентной модели расследований. Это закономерный шаг, позволяющий перейти к созданию масштабной системы расследований инцидентов ИБ и глубокой бизнес-аналитики корпоративных коммуникаций», — рассказывает Игорь Ляпунов, директор Центра информационной безопасности компании «Инфосистемы Джет».

Компаниям, использующим предыдущие релизы продукта, «Дозор-Джет» 5.0.4 доступен в режиме штатного обновления.

Новый Kaspersky Internet Security: частная жизнь останется частной

18 сентября 2014, Россия, Москва
Источник: kaspersky.ru



Kaspersky Internet Security

«Лаборатория Касперского» выпускает новую версию своего флагманского продукта для защиты пользователей Kaspersky Internet Security для всех устройств. Обновленное решение содержит не только инструменты противодействия киберугрозам, но и новые функции для обеспечения конфиденциальности частной жизни пользователя. К тому же была оптимизирована производительность решения – теперь его работа не сказывается на быстродействии компьютера.

Согласно исследованию, проведенному «Лабораторией Касперского» совместно с B2B International в 2014 г., электронные устройства – не просто гаджеты для выхода в сеть. Пользователи доверяют им свою личную жизнь, ценную информацию, даже деньги. По данным опроса, 68% российских пользователей хранят на устройствах особо конфиденциальную информацию и боятся, что кто-нибудь может увидеть ее. Еще 52% опасаются скрытой слежки через веб-камеру. А 79% регулярно совершают финансовые операции в интернете, вводя конфиденциальные банковские данные на разных веб-сайтах. Такое многообразие активностей, информации и устройств, безусловно, требует тщательной защиты.

К примеру, особый режим для совершения финансовых транзакций в сети – «Безопасные платежи» – теперь защищает от несанкционированного доступа не только браузеры и экран компьютера, но также буфер обмена данных. Это лишает злоумышленника шанса перехватить ценную информацию при передаче данных от пользователя к платежному сервису.

Еще одной новой функцией является защита веб-камеры. Не секрет, что одним из распространенных способов кибершпионажа является взлом веб-камеры и перехват изображений, которые она транслирует. Чтобы ценная информация, а также действия, которые человек совершает в зоне охвата камеры, не попали в руки злоумышленников, «Лаборатория Касперского» включила в новую версию своего продукта специальную функцию защиты от несанкционированного подключения к веб-камере. Новая технология отслеживает любые приложения, которые пытаются установить связь с веб-камерой, предупреждает пользователя о подобных попытках и в случае необходимости блокирует доступ к камере.

Большой риск потерять ценные данные исходит также от программ-шифровальщиков, которые не просто делают файлы нечитаемыми, но и требуют выкуп за восстановление доступа к информации. Эту проблему нельзя решить простым удалением вредоносной программы. Для повышения эффективности защиты от подобных угроз в Kaspersky Internet Security для всех устройств реализована улучшенная функция мониторинга активности. Теперь она не просто анализирует все процессы, происходящие в операционной системе, но в автоматическом режиме создает резервные копии файлов, которые имели контакт с подозрительной программой. Если информация претерпела вредоносные изменения, продукт автоматически восстановит резервную копию файла.

Еще один излюбленный прием злоумышленников – перехват данных через незащищенное соединение по Wi-Fi. Kaspersky Internet Security для всех устройств усложнит эту задачу: новая функция проверки безопасности публичных сетей Wi-Fi оценивает надежность и защищенность точки доступа и предупреждает пользователя в случае обнаружения потенциальной опасности. Также решение выдает пользователям советы и рекомендации по настройке безопасной сети Wi-Fi в собственном доме. Обновленное решение также осуществляет контроль интернет-трафика через сети Wi-Fi, 3G и 4G, что помогает пользователю оптимизировать расходы на мобильный интернет. А функция «Родительский контроль» теперь поддерживает безопасный поиск в социальной сети www.vk.com, благодаря чему ребенок сможет увидеть только те видеоролики, которые подходят ему по возрастным ограничениям. Наконец, каждый владелец девайса, на котором установлена новая версия Kaspersky Internet Security для всех устройств, может быть уверен в том, что используемое им защитное ПО содержит самые передовые технологии, поскольку процесс загрузки обновлений теперь стал автоматическим.

КОМПЕТЕНТНОЕ МНЕНИЕ:

Владимир Заполянский, Лаборатория Касперского, вице-президент по продуктовому и технологическому маркетингу

<<Современные пользователи уже достаточно хорошо осведомлены о киберугрозах, и сегодня мы видим, что они начинают по-настоящему переживать за сохранность своих ценных данных и опасаются любого вторжения в свою частную жизнь. Именно поэтому мы уделяем большое внимание созданию комплексной системы защиты, которая способна обеспечить высокую степень конфиденциальности и сохранности не только «цифрового мира» пользователя, но и его реальной жизни.>>

«Элвис-Плюс» разработала защищенный ноутбук для чиновников под присмотром ФСБ России

19 сентября 2014, Россия, Москва

Источник: pilaru.ru

ЭЛВИС-ПЛЮС

Компания Александра Галицкого «Элвис-Плюс» готовит к релизу защищенный ноутбук с технологией «Базовый доверенный модуль». Устройство адресовано потребителям из госструктур. Его разработка велась в соответствии с техзаданием, предварительно согласованным с ФСБ.

Зеленоградская компания «Элвис-Плюс» собирается вывести на рынок линейку защищенных отечественных устройств, работающих с использованием ее собственной технологии «Базовый доверенный модуль» (БДМ).

Как рассказал CNews директор департамента развития «Элвиса» Роман Кобцев, линейка защищенных устройств будет включать ноутбук, планшет, сервер, и, возможно, смартфон.

Ноутбук Lenovo с БДМ-функциональностью будет представлен в конце сентября 2014 г., БДМ-планшет и сервер компания рассчитывает вывести на рынок до конца 2015 г., а запуск БДМ-смартфона будет зависеть от результатов продаж первых продуктов линейки.

По заявлению компании, технология позволяет контролировать целостность операционной системы, ПО, системных файлов и пр., что обеспечивает защиту информации несанкционированного доступа при потере ноутбука или при попытках несанкционированного доступа.

Защищенная техника «Элвис-Плюс» адресована, главным образом, государственному заказчику, который уже выказал внимание к продукту. Дополнительный интерес к БДМ-устройствам проявили частные компании, что стало для разработчиков сюрпризом, говорит Роман Кобцев.

Названий госзаказчиков и коммерческих компаний, проявивших интерес к готовым ноутбукам Lenovo с БДМ, Роман Кобцев не раскрывает, как и объема закупок, который они хотели бы совершить. Свои расчеты емкости российского рынка защищенных устройств «Элвис» не раскрывает.

Из публикации газеты «Ведомости» известно о намерении госкорпорации «Ростех» приобрести 3000 защищенных ноутбуков для своих топ-менеджеров. В числе потенциальных поставщиков защитной технологии фигурировал «Элвис-Плюс» со своей разработкой. Роман Кобцев в разговоре с CNews интерес «Ростеха» к разработкам «Элвиса» подтвердил.

Аппаратная часть технологии БДМ основана на криптографическом чипе TPM (Trusted Platform Module, «Модуль доверенной платформы»), интегрированном в большинство современных ноутбуков.

Программная часть БДМ разработана в «Элвис-Плюс» и реализована с помощью российского криптографического алгоритма, описанного в ГОСТ 28147-89 и использования разрешенных защитных функций чипа безопасности.

По словам Романа Кобцева, вся разработка продукта велась в строгом соответствии с техническим заданием, предварительно согласованным с ФСБ.

Сейчас «Элвис-Плюс» находится в процессе получения своей разработкой сертификата ФСБ класса КС3, который, как ожидается, может быть им выдан до окончания 2014 г. Системы, сертифицированные по классу КС3, могут использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.

Интересно, что нынешний релиз «Базового доверенного модуля» в исполнении «Элвис-Плюс» - это уже второе за последние 10 лет появление защитной технологии под тем же названием, разработанной в той же компании.

В 2005 г. «Элвис-Плюс» уже презентовал защищенные мобильные ПК IBM, однако тогда работы над БДМ были прерваны вследствие покупки китайской Lenovo бизнеса IBM по производству ПК.

«Элвис-Плюс» на 58% принадлежит ИТ-предпринимателю и инвестору Александру Галицкому. В 1993 г. компания Sun Microsystems начала приобретение акций «Элвиса», сформировав пакет в 15%. Сейчас, после ряда дополнительных эмиссий, доля Oracle, поглотившей Sun в 2010 г., в «Элвис-Плюс» не превышает 1%.

Как пояснил CNews Роман Кобцев, «Элвис-Плюс» извещал Sun о допэмиссиях «Элвиса», «однако они не выразили желания принять в них участие».

Согласно отчетности компании, в 2013 г. ее выручка составила 930,8 млн руб., что несколько хуже, чем 997,6 млн руб. годом ранее. По данным IDC, компания входит в десятку игроков на российском рынке информационной безопасности в сегменте IT Security Services с долей около 3,3% при выручке в этом сегменте $17,04 млн.

По данным годового отчета «Элвис-Плюс» за 2013 г., доля компании в продаже услуг и поставках программных и аппаратных средств на российском рынке ИБ, по данным ее собственных аналитиков, составляла 7-8%.

В 2011 г. компания сообщала, что ее основные клиенты это госструктуры (около 60% оборота) и крупные компании (40%). Самым крупным клиентом «Элвис-Плюс» в 2011 финансовом году стал Центробанк, на который приходилось 11% оборота. Кроме того компания тогда назвала значимыми проекты в Росреестре, ФСТЭК, ФНС, Информационно-аналитическом центре правительства Санкт-Петербурга и «Ростелекоме». Всего у «Элвиса-Плюс» в 2011 г. было около 400 заказчиков.

«Рамэк» и «Газинформсервис» представили защищенные рабочие станции

23 сентября 2014, Россия, Москва
Источник: rosinvest.com

Компания «Рамэк» совместно с компанией «Газинформсервис», разработчиком программного обеспечения в области информационной безопасности, выпустила программно-аппаратные комплексы Ramec Safe и Ramec EFROS.

Как сообщили CNews в «Рамэк», Ramec Safe представляет собой ПАК, состоящий из рабочей станции семейства Ramec GALE и предустановленных сертифицированных средств защиты информации. Он предназначен для комплексной и многофункциональной защиты информационно-программных ресурсов от несанкционированного доступа. ПАК Ramec Safe уже содержит

в своем составе сертифицированный межсетевой экран и аппаратный модуль доверенной загрузки операционной системы.

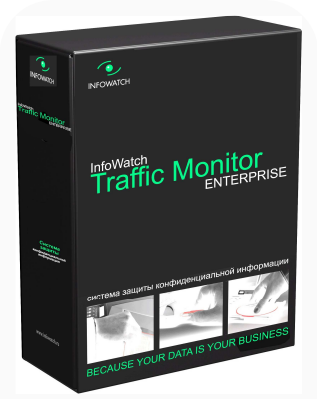
По информации «Рамэк», Safe обеспечивает разграничение доступа по средствам двухфакторной аутентификации пользователя, возможность аудита событий, выполнение требования ФЗ №152 «О персональных данных». Защищенные рабочие станции Ramec Safe будут полезны всем компаниям, выполняющим обработку персональных данных, так как они выступают операторами (согласно закону РФ «О персональных данных»).

В свою очередь, ПАК Ramec EFROS предназначен для активного аудита сетевого и серверного оборудования. Он позволяет вести постоянный контроль неизменности конфигураций и хранить их на протяжении жизненного цикла корпоративной инфраструктуры.

В целом Ramec EFROS обеспечивает: контроль конфигураций всех узлов инфраструктуры; уменьшение времени восстановления при отказе оборудования, так как все настройки сохранены в БД; соблюдение требований руководящих документов РФ в части контроля целостности. Решение отличает широкий спектр поддерживаемого оборудования (в том числе производства 3Com Corporation, РКСС, «С-Терра СиЭсПи», VMware, HP, Crossbeam, Oracle). ПАК EFROS в Ramec рекомендуют компаниям, имеющим в своей инфраструктуре значительный парк сетевого/серверного оборудования.

InfoWatch представила свои новые разработки в области защиты информации от внутренних угроз

23 сентября 2014, Россия, Москва
Источник: infowatch.ru



InfoWatch Traffic Monitor Enterprise

Компания InfoWatch представила свои новейшие разработки в области защиты информации от внутренних угроз. Как сообщили CNews в InfoWatch, компания впервые продемонстрировала концепт-версию DLP-решения InfoWatch Traffic Monitor Enterprise, которая способна анализировать SMS-трафик и фотографии, сделанные при помощи мобильного устройства, на наличие в них конфиденциальной корпоративной информации.

По словам разработчиков, представленная функциональность «мобильного DLP» призвана защитить данные на мобильных устройствах и решить проблему BYOD. Вкупе с уже имеющимися широкими возможностями гибридного анализа, данная технология позволит InfoWatch Traffic Monitor Enterprise обеспечить контроль максимального числа каналов, включая и те, которые ранее оставались недоступными для систем защиты от внутренних угроз, подчеркнули в InfoWatch.

Кроме того, компания продемонстрировала решение InfoWatch Targeted Attack Detector, которое было анонсировано в апреле 2014 г. В основе решения лежит технология динамического анализа. Принцип работы технологии основан на постоянном, протяженном во времени процессе сканирований критических элементов ИТ-системы с последующим анализом произошедших изменений на предмет аномалий. Благодаря этой технологии атака может быть обнаружена на самой ранней стадии, что снижает риск компрометации ИТ-систем компаний, указали в InfoWatch.

Компания также представила решение InfoWatch Personal Data Protector, ориентированное на защиту персональных данных. Концепция решения была разработана с учетом того, что большая часть информации, утекающей из СМБ-компаний, приходится именно на персональные данные, и именно их защите регулирующие органы уделяют особое внимание.

SearchInform представила новые и обновленные решения для предотвращения утечек данных

25 сентября 2014, Россия, Москва
Источник: searchinform.ru

Компания SearchInform представила новые и обновленные компоненты своего флагманского решения «Контура информационной безопасности SearchInform».

Так, новый модуль ViberSniffer предназначен для мониторинга трафика приложения для обмена сообщениями Viber. Особенностью ViberSniffer является перехват всей инфор-

мации: чатов, звонков, файлов и контактов. С учетом полной синхронизации десктопной и мобильной версий Viber, отдел информационной безопасности получает огромное количество новых данных для анализа, в том числе и полные телефонные книги пользователей. За счёт интеграции ViberSniffer в AlertCenter специалистам отдела информационной безопасности доступны все аналитические возможности «Контура информационной безопасности SearchInform», включая запатентованный алгоритм «Поиск похожих», рассказали в компании.

По информации SearchInform, претерпели изменения и уже зарекомендовавшие себя, продукты компании. Так, в решении SearchInform MonitorSniffer появился реализованный по многочисленным пожеланиям клиентов режим непрерывной записи действий сотрудников. По словам разработчиков, за счёт применения захвата изображения по ключевым кадрам вкупе с передовыми алгоритмами сжатия удалось достичь экономии при сохранении информации. Так, 4 часа непрерывного «кино» занимают порядка 150 МБ. При этом файл с записью можно просмотреть на любом компьютере в стандартном медиапроигрывателе, то есть без специального «клиента-просмотрщика».

В свою очередь, обновлённый SearchInform DeviceSniffer теперь поддерживает автоматическое шифрование всей информации, записываемой на внешние носители. На всех компьютерах корпоративной сети, где установлен DeviceSniffer, зашифрованные данные откроются без каких-либо затруднений для пользователя, в то время как сторонний человек, получив подобную флэшку, увидит лишь зашифрованные данные. Для обеспечения легальной передачи данных удаленным контрагентам предусмотрен режим удаленной разблокировки. Такой простой механизм обеспечивает защиту конфиденциальной информации компании как от преднамеренных, так и от случайных утечек, подчеркнули в SearchInform.

В свою очередь, оптимизированная интеграция URLSniffer с инструментом отчётности SearchInform ReportCenter теперь позволяет не только построить отчет обо всех посещённых сотрудником сайтах и проведённом на них времени, но и автоматизировать этот процесс. Так, с помощью мастера отчётов можно создать автоматическое оповещение, к примеру, о том, что сотрудник провёл на страницах соцсетей слишком много (более 30 минут) времени в течение рабочего дня. Это позволяет выявлять сотрудников, расходующих оплаченное работодателем время нецелевым образом.

Как отметил генеральный директор компании SearchInform Лев Матвеев, «новые функции "Контура информационной безопасности SearchInform" позволят компаниям выстроить еще более эффективную систему защиты от утечек конфиденциальной информации и обезопасить себя от возможных убытков».

«Актив» начал продажи «Рутокен ЭЦП Bluetooth»

25 сентября 2014, Россия, Москва
Источник: rutoken.ru

Компания «Актив» начала продажи устройства «Рутокен ЭЦП Bluetooth». Как сообщили CNews в «Активе», решение предназначено для безопасного хранения и использования ключей шифрования и электронной подписи на мобильных устройствах на базе iOS и Android.

По информации компании, «Рутокен ЭЦП Bluetooth» можно одинаково эффективно использовать как на ПК и ноутбуках на базе ОС Windows, Linux и OS X, подключив через USB-порт, так и на мобильных устройствах на базе Android и iOS благодаря поддержке Bluetooth. «Рутокен ЭЦП Bluetooth» создан с учетом строгих государственных требований в области информационной безопасности, поддерживает российские стандарты электронной подписи, шифрования и хеширования, что делает его универсальным электронным идентификатором. Криптографические операции выполняются внутри самого токена, что повышает защищенность информационной системы. Его использование не требует специальных знаний: необходимо просто подключить токен к компьютеру или установить соединение с мобильным устройством через Bluetooth и начать работать. Также не нужно беспокоиться об утечке ключевой информации через Bluetooth: в устройстве предусмотрено шифрование Bluetooth-канала по государственному стандарту ГОСТ 28147-89, рассказали в компании.

Кроме того, разработчики средств информационной безопасности оценят кроссплатформенный интерфейс PKCS#11, позволяющий легко интегрировать «Рутокен ЭЦП Bluetooth» в их решения. Ознакомиться со всеми возможностями «Рутокена ЭЦП Bluetooth» можно с помощью специально разработанного клиентского приложения, которое доступно в Google Play. Приложение для iOS будет доступно в ближайшее время.

Устройство выполнено в стильном корпусе. Решения «Рутокен ЭЦП Bluetooth» поставляются в индивидуальной упаковке. В комплект поставки входят USB-провод для подключения к компьютеру и шнурок для удобного ношения. По желанию заказчика может быть выполнено брендирование токена: логотип, нанесенный на корпус методом тампопечати, придаст устройствам индивидуальность и сделает их узнаваемыми. С сентября «Рутокен ЭЦП Bluetooth» доступен не только в белом, но и в черном корпусе с матовым покрытием «софт тач».

Gemalto представила новое приложение для совершения безопасных онлайн-платежей

30 сентября 2014, Нидерланды
Источник: anti-malware.ru

Компания Gemalto представила новое решение Ezio Armored Application — приложение, которое позволяет банкам в короткие сроки устанавливать безопасные программы для осуществления онлайн-платежей на любой компьютер. Ezio Armored Application защищает всех пользователей, которые совершают платежи в режиме онлайн, от кибератак и мошеннических схем последнего поколения, сообщили CNews в Gemalto.

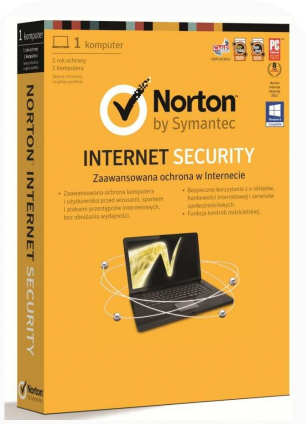
По словам разработчиков, решение Ezio Armored Application, которое работает в режиме защищенной веб-страницы в отдельной пользовательской сессии, обеспечивает безопасное подключение к сайту, на котором будет совершен онлайн-платеж и предотвращает любую утечку информации. Такой механизм работы программы существенно затрудняет проведение кибератак типа «человек-в-браузере» (man-in-the-browser) или «человек посередине» (man-in-the-middle). Кроме того, программа тщательно анализирует ступень безопасности ИТ-инфраструктуры со стороны конечного пользователя, оценивает возможные риски кибератак и при необходимости осуществляет сбор данных для дальнейшего анализа.

В то же время, новое решение Gemalto для банков также способствует более активному использованию инструментов онлайн-банкинга конечными пользователями. Для того чтобы установить Ezio Armored Application на компьютере, пользователю необходимо просто пройти по ссылке и загрузить приложение. При этом использовать сам портал онлайн-банкинга так же просто, как работать с обычным веб-браузером, утверждают в компании.

«Мы разработали данное решение, опираясь на наш значительный опыт работы с клиентами в банковской сфере по всему миру. Мы постоянно адаптируем наши решения в зависимости от потребностей конкретного рынка и угроз, с которыми приходится сталкиваться нашим клиентам в разных странах, — рассказал Хёган Нордфйель, первый вице-президент департамента онлайн-банкинга и электронной коммерции компании Gemalto. — Мы предоставляем нашим клиентам весь спектр решений Gemalto, в который входят как программное обеспечение в сфере безопасности, так и другие решения. Наши продукты обеспечивают банки необходимыми инструментами для управления рисками. Новое решение Gemalto дополняет наш портфель решений для онлайн-банкинга и позволяет адаптировать наше предложение в зависимости от потребностей клиента».

Symantec обещает вернуть деньги за Norton Security, если он не справится с вирусами

30 сентября 2014, США
Источник: mir.ufanet.ru



антивирусное ПО Norton

В России стартовали продажи обновленной линейки антивирусного ПО Norton компании Symantec. Вместо девяти продуктов конечным пользователям предложено одно решение в двух редакциях. Если оно не справится со зловредами, Symantec обещает вернуть деньги, выплаченные за подписку.

В России начались интернет-продажи анонсированного месяц назад нового флагманского решения Symantec — Norton Security. Оно пришло на смену девяти ранее существовавшим основным продуктам компании для конечных пользователей: Antivirus, Internet Security, 360 и др.

Как сообщил в разговоре с CNews Олег Никитский, руководитель подразделения Norton в России, странах СНГ, Швейцарии, Польше, Чехии и Словакии, отказ от разветвленной линейки произошел в интересах пользователей.

«Девять продуктов покрывали различные потребности клиентов в защите — базовые, расширенные, с бэкапом, с утилитами и пр. И людям, особенно тем, кто не сильно разбирается в компьютерах, достаточно сложно было понять, что же им действительно нужно, какую защиту выбрать», — говорит он.

Теперь в компании предлагают клиентам просто приобретать решение с максимальной защитой и ни о чем больше не беспокоиться. Его универсальность также выражается в кросс-платформенности — пользователь по одной лицензии может защитить сразу несколько своих устройств: PC и Mac, а также смартфоны и планшеты на Android и iOS.

Несмотря на то, что новое решение доступно и в коробке, концептуально Norton Security позиционируется как сервис — подписка на него покупается на год.

На российском сайте компании решение продается в двух версиях. При защите до 5 устройств в год цена составляет 1799 руб.. За этот же продукт, покрывающий до 10 устройств и предоставляющий воз-

можность резервного копирования файлов в 25-гигабайтном облачном хранилище, заплатить придется 2599 руб.. Для сравнения, стоимость Norton Internet Security на 1 год, на 3 ПК составляла 1590 руб.

Уровень цен на коробочную версию новинки станет известен лишь в начале ноября. Именно тогда Norton Security появится в российском ритейле. По словам Никитского, розница отнеслась к новшеству Symantec весьма позитивно — проще закупать и расставлять на полках один продукт, а не девять, да и продавцам легче продавать одну коробку одного производителя, не тратя время на сравнительные консультации.

Глава представительства Symantec в России и СНГ Андрей Вышлов уточнил CNews, что в обозримом будущем Norton Security начнет продаваться в интернете у партнеров компании и у сервис-провайдеров. Также планируется предустанавливать его на устройства партнеров Symantec.

При позиционировании торговой марки Symantec решила использовать маркетинговый ход, связанный с обещанием вернуть клиенту деньги, если Norton Security не убережет его устройство от проникновения зловредного кода, а служба поддержки впоследствии не сумеет устранить проблему. По утверждению Никитского, таких обязательств на себя не брала еще ни одна компания в мире.

Правда, нужно понимать, что претендовать на такой формат обслуживания смогут лишь пользователи, соглашающиеся на продление продукта с ежегодным автоматическим списанием соответствующей суммы с кредитной карты. Никитский заверяет, что подобных клиентов у Symantec в России немало, но конкретные цифры не раскрывает.

Система обнаружения компьютерных атак «Форпост» на серверной платформе «Аквариуса» поступила в продажу

01 октября 2014, Россия, Москва
Источник: gigamir.net

Система обнаружения компьютерных атак «Форпост»

В продажу поступили новые версии программно-аппаратных комплексов (ПАК) «Форпост 200» и «Форпост 2000», предназначенных для обнаружения компьютерных атак, на серверных платформах серии Telecom от компании «Аквариус», отечественного производителя компьютерной техники. Об этом CNews сообщили в компании РНТ, российском системном интеграторе и разработчике сертифицированных средств защиты информации.

Серверы Aquarius Server T40 S23 и Aquarius Server T50 D15, используемые при производстве изделий ПАК «Форпост 200» и ПАК «Форпост 2000», обеспечивают требуемую производительность благодаря тщательно подобранной конфигурации, 100% входному контролю компонентов и многоэтапным 72-часовым испытаниям готовой продукции, отметили в РНТ. Они оптимизированы для использования в стойке, занимают минимум пространства и обеспечивают хорошую доступность при проведении сервисных работ, указали в компании.

Как пояснили в РНТ, выбор «Аквариуса» в качестве поставщика серверных платформ обусловлен должным качеством продукции, что важно в производстве решений информационной безопасности. «Новые продукты как результат сотрудничества двух российских компаний — это в том числе наш отклик на решения Правительства РФ по обеспечению технологической независимости России и замещению импортной продукции», — заявили в компании.

По информации РНТ, система обнаружения компьютерных атак (СОА) «Форпост» версии 2.0 предназначена для автоматического выявления воздействий, которые могут быть классифицированы как компьютерные атаки, на контролируемую данным средством автоматизированную информационную систему, блокирования развития выявленных компьютерных атак. «Форпост» может поставляться как программный продукт или программно-аппаратное решение «в одной коробке». В линейке продуктов «Форпост» доступен также программный комплекс «Форпост-Мониторинг», предназначенный для отслеживания состояния контролируемых ресурсов автоматизированной информационной системы и разбора ситуаций в случае возникновения проблем с доступностью к ИТ-сервисам.

СОА «Форпост» применяется в органах государственной власти РФ в автоматизированных информационных системах, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну (в соответствии с требованиями ФСБ России), а также в информационных системах, в которых обрабатывается информация, содержащая секретные сведения (в соответствии с требованиями ФСТЭК России — в автоматизированных системах до класса защищенности 1В включительно, информационных системах персональных данных до 1 класса включительно).

«Крок» представил облачную услугу информационной безопасности

02 октября 2014, Россия, Москва
Источник: cloud.croc.ru

Компания «Крок» разработала облачную услугу информационной безопасности Security-as-a-Service (SecaaS) на основе сертифицированных средств защиты информации. Об этом CNews сообщили в «Крок».

Для предоставления новой услуги в «облаке» «Крок» создал централизованный узел безопасности (ЦУБ), на основе которого может быть построена защита информационной системы персональных данных в соответствии с индивидуальной моделью угроз заказчика. Аренда облачного сервиса позволит российским компаниям снять с себя ряд вопросов по созданию и эксплуатации системы защиты, обезопасив бизнес от штрафов и остановок путем минимальных временных и финансовых затрат. Развернуть требуемые сервисы информационной безопасности в ЦУБ «Крок» можно в течение 1-2 дней.

«Многие наши заказчики в соответствии с требованиями регуляторов для защиты своих систем должны использовать только сертифицированные средства информационной безопасности. Это, прежде всего, коммерческие компании, работающие с персональными данными. Поэтому даже в том случае, когда облачная модель потребления ресурсов была им удобна, воспользоваться ей они не могли. Сейчас сертифицированные средства защиты можно использовать не только при размещении системы в облачном ЦУБе "Крок", но и в случае аренды ресурсов в одном из наших дата-центров. Этой услугой уже заинтересовались первые заказчики, из отраслей страхования и медицины», — рассказал Михаил Башлыков, руководитель направления информационной безопасности компании «Крок».

Технически новая услуга представляет собой защищенную виртуальную среду с сервисами информационной безопасности, построенными на базе инструментов, сертифицированных ФСТЭК и ФСБ России. К их числу относятся средства межсетевого экранирования, криптографической защиты каналов связи (IPSec VPN) и предотвращения вторжений (IPS).

ИНДИКАТОРЫ РАЗВИТИЯ. АНАЛИТИКА. ОБЗОРЫ. ЭКСПЕРТНЫЕ ОЦЕНКИ

Глава Роскомнадзора прокомментировал ситуацию с утечками в интернет пользовательских идентификаторов популярных почтовых сервисов

12 сентября 2014, Россия, Камчатский край
Источник: iksmedia.ru

Александр Жаров, Глава Роскомнадзора

Глава Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Александр Жаров завершает рабочую поездку по Дальневосточному федеральному округу.

12 сентября руководитель Роскомнадзора встретился в Петропавловске-Камчатском с губернатором Камчатского края Виктором Илюхиным. На встрече обсуждалось развитие связи и массовых коммуникаций в регионе, а также вопросы взаимодействия краевого управления Федеральной службы с различными органами власти на региональном уровне.

Ранее Жаров посетил Сахалинскую область и Приморский край.

Отвечая на вопросы камчатских журналистов, Александр Жаров прокомментировал резонансные темы, связанные с регулированием интернета.

Говоря об утечках идентификационных данных пользователей популярных почтовых сервисов, он отметил: «К сожалению, взломы публичных почтовых или облачных сервисов – явление сегодня довольно распространенное. Как показывает практика, эффективной защитой своих сервисов от хакеров не может похвастаться ни один интернет-гигант – будь то «Яндекс», Mail.ru или Google. Роскомнадзор как уполномоченный орган по защите персональных данных россиян внимательно следит, чтобы личная информация граждан не оказывалась в открытом доступе. По факту последних «громких» утечек почтовых паролей в интернет в Роскомнадзор поступило около двух десятков обращений граждан.

Надо сказать, что в терминологии действующего законодательства логины и пароли электронной почты или аккаунтов в социальных сетях не являются персональными данными. Поэтому у нас нет законных оснований для проведения каких-либо проверок в отношении интернет-компаний, допустивших утечки. Другой вопрос, что получив доступ к почтовым идентификаторам, злоумышленники получают в свое

распоряжение содержание вашей переписки – где, конечно, могут быть и ваши персональные данные: изображения, контактная информация, пересылаемые документы и т.д. Наша задача – оперативно выявить, когда такая информация появится в Сети, и прекратить ее распространение.

Сейчас мы активно используем практику прекращения распространения персональных данных россиян в судебном порядке. За последние месяцы суды вынесли соответствующие решения об ограничении доступа к 12 сайтам-нарушителям законодательства о персональных данных, исковые заявления Роскомнадзора в отношении более 60 сайтов находятся в стадии судебных разбирательств. Отрадно, что в двух случаях суды вынесли определения о предварительных обеспечительных мерах – такая практика позволяет нам добиваться от интернет-ресурсов удаления персональных данных до того, как длительное судебное разбирательство будет завершено, и в течение месяца решение суда вступит в законную силу. В случае с персональными данными скорость нашей реакции критична, ведь всегда существует риск, что ваша личная информация будет использована преступниками, и возникнет угроза вашей физической безопасности, здоровью, жизни или репутации».

75% приложений на гаджетах сотрудников опасны для работодателей

16 сентября 2014, США
Источник: inform.kz

Лишь одно из каждых четырех мобильных приложений удовлетворяет требованиям корпоративной безопасности, указывают эксперты. По их словам, с учетом темпов распространения мобильных технологий предприятиям следует в обязательном порядке внедрять механизмы тестирования приложений и страхования от рисков.

Более 75% мобильных приложений не удовлетворяют базовым требованиям корпоративной безопасности, сообщила исследовательская компания Gartner. Аналитики предупредили, что такая ситуация сохранится как минимум до конца 2015 г.

В компании прогнозируют, что в 2014 г. пользователями во всем мире будет загружено на мобильные устройства почти 139 млрд приложений. К 2017 г. это значение вырастет почти до 269 млрд.

«Предприятия, пользующиеся мобильными устройствами или внедряющие стратегию «принеси свое собственное устройство» (Bring Your Own Device — BYOD), остаются уязвимы к нарушениям защиты, пока они не внедрят методы и технологии тестирования мобильных приложений на безопасность и не воспользуются страхованием от рисков, — заявил старший аналитик Gartner Дионисио Зумерли (Dionisio Zumerle).

Сегодня свыше 90% предприятий, внедряющих стратегию BYOD, пользуются сторонними мобильными приложениями. Поэтому так важно использовать механизмы проверки этих приложений, подчеркнул эксперт.

Аналитики поясняют, что сегодня разработчики в основном посвящают свое время функциональности мобильных приложений и не уделяют внимания их безопасности. Поэтому риски, связанные с использованием таких программ, обусловлены по большей части не действиями злоумышленников, а отсутствием в этих приложениях какого бы то ни было бережного отношения к данным.

Согласно Gartner, в период до 2017 г. включительно 75% нарушений защиты мобильных приложений будут связаны с неправильной работой этих приложений, а не с атаками на мобильные устройства. В качестве примера аналитики приводят приложение для доступа к какому-либо бесплатному облачному сервису, в которое случайно могут попадать корпоративные данные, хранящиеся на смартфоне. Такая ситуация может привести к утечке коммерческих секретов.

Однако и хакерские атаки приобретут большее значение. Аналитики прогнозируют, что в ближайшие годы количество атак на мобильные устройства продолжит возрастать. Уже сейчас оно втрое превышает количество атак на рабочие станции.

Данные Gartner подтверждаются и другими исследованиями. В конце 2013 г. похожий отчет был выпущен исследовательским подразделением крупнейшего в мире производителя серверов и второго по величине поставщика персональных компьютеров Hewlett-Packard. Согласно HP Security Research, 86% мобильных приложений не содержат адекватных механизмов защиты от атак и утечек информации.

"Халатность пользователей становится самым слабым звеном"

16 сентября 2014, Россия, Москва
Источник: astera.ru

Интервью с Алексеем Лукацким, бизнес-консультантом по безопасности компании Cisco.

Вопрос: Информационная безопасность. Какие новые угрозы вы могли бы назвать? Как им противостоять?

Ответ: Я бы не сказал, что сейчас появляются кардинально новые угрозы, которых не было раньше. Никакой революции не происходит, скорее всего, это эволюционное развитие. Меняется зачастую поведение как пользователей, которые становятся все более беспечными ввиду массового развития информационных технологий, так и поведение злоумышленников, которые ориентируются уже не на массовое

распространение вредоносных программ или каких-то угроз, а фокусируются на одну компанию или группу компаний, объединенных по каким-то принципам. Это позволяет злоумышленникам оставаться гораздо дольше незамеченными и получать больший результат от действий своих вредоносных программ, несмотря на то, что они не такие массовые, при этом показатель заражения измеряется не долями, а может доходить до нескольких десятков процентов. И еще одна тенденция, скорее всего, не революционная, а эволюционная - это использование злоумышленниками в целях проникновения в те или иные системы не одного вектора, а сразу нескольких уязвимостей, векторов, каналов проникновения. Все это является тенденцией на сегодняшний день с точки зрения злоумышленников, и, как следствие, компании, которые занимаются защитой как собственной организации, так и других компаний, должны учитывать эти тенденции. Уже, к сожалению, нельзя использовать одно точечное решение, как это было раньше - поставили межсетевой экран на периметре, установили антивирус на рабочей станции или на сервере, и как бы они решают все проблемы ИБ. Не решают! В корпоративную сеть или сеть оператора связи можно попасть разными способами: и через межсетевой экран (традиционный вариант), и через флешку, и с помощью компакт-диска, и по электронной почте, и через 3G- или 4G-модем, который сотрудник подключил к своему компьютеру, и через левую точку беспроводного доступа, и через синхронизацию ActiveSync, и т.д. Вариантов огромное количество. И, как следствие, одно средство защиты уже не спасает. Оно обходится элементарно, необходимо использовать комплексную систему, как бы старо это не звучало, это должен быть некий комплекс из различных технологий, продуктов, установленных в разных местах, которые позволяют, с одной стороны, выстроить некую эшелонированную "стену" вокруг защищаемой системы, т.е. бороться с атаками до их появления на периметре организации. С другой стороны, мы должны быть готовы, что атаки все-таки могут использовать слабые места системы защиты, таким образом, мы должны обнаруживать несанкционированные действия в процессе их реализации. И, наконец, третье, самое важное, что отличает текущий день от прежних - мы должны быть готовы, что какие-то угрозы все-таки заразят или скомпрометируют отдельные узлы, может произойти компрометация узлов, утечка информации. И задача специалиста по безопасности - не закрывать на это глаза, а признать такую проблему и как можно скорее локализовать ее, не давая распространяться по организации, т.е. провести расследование, изучить сетевой трафик, увидеть индикатор, говорящий о компрометации и, тем самым, своевременно идентифицировать источник проблемы, ограничить его и затем привести систему в предатакованное состояние. То, что сейчас происходит, эпизодически происходило и ранее, но сейчас стало носить все более массовый характер, потому что со старыми методами борьбы эффективно построить систему защиты невозможно.

Алексей Лукацкий, бизнес-консультантом по безопасности компании Cisco.

Вопрос: Подход к информационной безопасности в России и в мире. Есть ли существенные отличия? На какие нюансы информационной безопасности обращают внимание российские компании?

О: Отличия есть, они касаются, в первую очередь, подходов к регуляторике. Практически в каждой стране мира есть свои обязательные требования по обеспечению ИБ, но у нас их количество завышено. Как следствие, реальное обеспечение безопасности подменяется необходимостью выполнения бумажных требований регуляторов. И многие компании ищут не решения своих реальных проблем, а способ успешно пройти проверку со стороны регулятора. Вот в этом, наверное, ключевое отличие России от западных и ряда восточных стран, потому что там акцент делается на реальной безопасности, влияние регуляторов существенно ниже, чем в России, а если оно и есть, то касается либо критических отраслей, критически важных объектов, либо государственного сектора, причем тоже не всего (обработка специфической информации, гостайна либо некоторые промежуточные уровни до общедоступной информации). У нас, к сожалению, регуляторы больше контролируют, чем во всем мире. И индивидуальный предприниматель, и монополист вроде Газпрома или РЖД попадают под прицел регулятора, что не всегда, на мой взгляд, является правильным подходом. И второе отличие, как следствие первого, заключается в том, что российский рынок разработчиков средств защиты информации также ориентирован на регуляторику. Если на западе продукты разрабатываются исходя из потребностей заказчика, рынка, то у нас - из потребностей регулятора. Именно поэтому продуктов российской разработки у нас немного, а те, что есть на сегодняшний день, как правило, реализуют устаревшие требования нормативных документов регуляторов, которые не всегда помогают решать бизнес-задачи. Но ситуация потихоньку меняется, сейчас стали появляться стартапы. В частности, наше сотрудничество с фондом "Сколково", участие в организуемых фондом мероприятиях показывают, что там за последние 2-3 года было создано несколько десятков стартапов по ИБ. Это очень хороший показатель, это значит, что у российских средств защиты есть будущее, есть перспектива занять свою нишу как внутри страны, так и за ее пределами. В остальном же серьезных отличий на сегодняшний день я не вижу.

<< ...Единственное, что хотелось бы, чтобы сами регуляторы не запрещали применения инновационных технологий безопасности, для которых у них еще нет своих требований... >>

В.: Какое место займет информационная безопасность в эру "всеобъемлющего интернета"?

О.: Как следствие, когда мы говорим об "интернете вещей", "всеобъемлющем интернете" как следующей стадии развития "интернета вещей", возникают вопросы: как защитить информацию, исходящую, например, с кардиостимулятора к домашнему доктору; как защитить информацию, получаемую автомобилем в режиме реального времени от датчиков, которые сигнализируют о пробках, мокром дорожном по-

крытии? Получается, что если злоумышленники вмешаются в этот процесс, то я попаду либо в пробку, либо меня занесет, потому что я не учту скоростной режим. Либо мой кардиостимулятор, не дай Бог, выдаст мне заряд тока, посчитав, что следует запустить встроенный дефибриллятор, приняв действия злоумышленника за сбой в ритме работы сердца. И такие примеры уже были. Все это кажется фантастикой, но элементы "всеобъемлющего интернета" стали появляться в нашей жизни уже сейчас. Недавно был прецедент, когда злоумышленники вывели из строя мультиварку и кофеварку путем их дистанционного включения через интернет. В кофеварке не было воды, а в мультиварке - продуктов. Все это привело к возгоранию. Вот вам пример недооценки обеспечения ИБ. Другой пример - Smart TB со встроенной видеокамерой, которая позволяет злоумышленникам наблюдать, что происходит в частной квартире. Соответственно, возникает необходимость защитить это межмашинное взаимодействие, которое составляет основу "всеобъемлющего интернета".

Учитывая, что интернет действительно всеобъемлющ, и то, что мы до сих пор до конца не можем предположить, куда еще встроят поддержку интернет-функций, мы должны думать о безопасности как самих элементов "всеобъемлющего интернета", так и их взаимодействия. Компания Cisco не всегда может повлиять на включение в стандарты межмашинного взаимодействия, "всеобъемлющего интернета" вопросов безопасности, не может повлиять на производителей различных устройств (кофеварок, холодильников, подгузников, которые тоже есть с подключением к интернету), поэтому наша задача хотя бы обеспечить защищенное взаимодействие между этими элементами. Поэтому мы наши технологии безопасности, которые очень хорошо восприняты на корпоративном рынке, модифицируем для того, чтобы их можно было применять во "всеобъемлющем интернете". Задачи примерно те же, но немного различаются способы их реализации. Но нам как компании, занимающейся разработкой сетевых технологий, протоколов, способов коммуникаций и сетевого оборудования, на которых строится "всеобъемлющий интернет", гораздо проще реализовывать многие вопросы, связанные с информационной безопасностью и интернетом вещей, чем другим игрокам этого рынка.

<<...Если на западе продукты разрабатываются исходя из потребностей заказчика, рынка, то у нас - из потребностей регулятора...>>

В.: Безопасность облака. Последние месяцы ознаменованы несколькими крупными утечками из облака (в том числе утечки личных фотографий знаменитостей). С чем, на ваш взгляд, это связано? С появлением новых киберугроз или с низкой цифровой грамотностью пользователей?

О.: Мы еще до конца не знаем, откуда утекли те самые фото знаменитостей, но, на мой взгляд, это связано с невысокой грамотностью в области ИБ рядовых интернет-пользователей. Они зачастую выбирают для своих интернет-ресурсов банальные, легко угадываемые пароли, а если пароли более или менее надежны, то они едины для всех аккаунтов и устройств пользователя, будь то электронная почта, облако, социальная сеть, домашний компьютер, и меняются очень-очень редко. Бывает, что эти пароли не меняются годами. Как следствие, именно эта халатность пользователей, а не системы защиты облачных платформ, которые атакуют и из которых осуществляются утечки, становится самым слабым звеном. Разумеется, бороться с этими угрозами нужно. Помимо необходимости повышения грамотности пользователей, существуют технологии анализа аномальной активности, обнаружения мошенничества в интернете, в том числе на облачных платформах, но эти технологии пока не получили широкого распространения ввиду недооценки этой проблематики. Зачастую сами владельцы облачных платформ пытаются переложить многие проблемы на пользователей вместо того, чтобы заниматься защитой своей инфраструктуры, поэтому это задача двусторонняя. Пользователи должны заниматься своей ИБ, а облачные платформы должны уходить от набора традиционных механизмов защиты в сторону существующих на рынке инновационных технологий.

В.: Изменения в регуляторных требованиях к защите информации. Каким требованиям должны соответствовать решения для информационной безопасности будущего?

О.: Наверное, ни в одной стране мира эта работа на опережение не реализована, и, пожалуй, она не нужна, потому что технологии настолько многообразны, что попытаться предвидеть их на уровне не просто "такое может быть", а на уровне конкретных требований, предъявляемых к этой технологии, довольно бесперспективно, поэтому за эту работу никто не берется, в том числе и в России. Единственное, что хотелось бы, чтобы сами регуляторы не запрещали применения инновационных технологий безопасности, для которых у них еще нет своих требований. Если этот баланс будет соблюден - когда возможно применение такого рода технологий, а со временем регулятор выработает для них свои требования, то это позволит эффективнее развиваться рынку ИБ.

В г. Алушта завершила работу XIII всероссийская конференция "Информационная безопасность. Региональные аспекты. ИнфоБЕРЕГ-2014"

17 сентября 2014, Россия, Крым респ.
Источник: itsec.ru

ИнфоБЕРЕГ 2014

Центральное место в программе конференции заняли вопросы развития нормативно-правовой базы в сфере ИБ и тема импортозамещения.

В конференции приняли участие более 200 руководителей и специалистов по информационным технологиям, информационной и экономической безопасности из 40 субъектов РФ, представляющих телекоммуникационную отрасль, предприятия топливно-энергетического комплекса и

промышленности, финансовые учреждения и другие компании с развитой ИТ-инфраструктурой.

В пленарной части конференции с приветственными словами выступили представители Министерства энергетики РФ, Министерства транспорта РФ, НП НПС, Академии Информационных Систем. Александр Павлович Баранов, ФГУП ГНИВЦ ФНС России, выступил с докладом, в котором он ввел понятие "массовой информационной безопасности" и характерные для нее проблемы. Среди которых: смешение государственной и гражданской ИБ, недостаточная грамотность населения в части ИБ, "тяжелые" механизмы по расследованию инцидентов и пр.

— В этом году конференция "ИнфоБЕРЕГ" впервые прошла в новом субъекте Российской Федерации — Крымском федеральном округе, - комментирует Андрей Николаевич Люльченко, президент ГК "СпецПроект". - Как известно, перед этим регионом в настоящее время остро стоит вопрос по созданию современной информационной инфраструктуры, отвечающей актуальным требованиям информационной безопасности. И я убежден, что те идеи и предложения, которые были выработаны в ходе нашей конференции, поспособствуют скорейшему решению этой задачи. Огромное спасибо Академии Информационных Систем за теплый прием и высокий уровень организации мероприятия.

Особое место в программе мероприятия заняла в этом году секция "Нормативное и правовое регулирование защиты информации в информационных системах", ведущими которой выступили Виталий Сергеевич Лютиков, ФСТЭК России, и Юрий Иванович Аксененко, ООО "ЦБИ". В секции приняли участие специалисты, участвовавшие в разработке нормативных и методических документов ФСТЭК России. Участники конференции особо отметили выступление Александра Петровича Глухова, ОАО "РЖД": "Опыт реализации мер защиты информации в автоматизированных информационных и телекоммуникационных системах ОАО "РЖД". По итогам проведения секции состоялась дискуссия и сбор предложений для ФСТЭК России от участников коференции.

С другой инициативой выступил Андрей Валерьевич Бугаенко, заместитель директора ФГУП НИИ "Восход", на секции по импортозамещению. В своем выступлении он сформулировал некоторые принципы формирования рынка с учетом тренда замещения зарубежных разработок разработками отечественными. В конце своего выступления он призвал участников присоединиться к разработке официального предложения об установлении и использовании заявленных принципов для Минкомсвязи России по регулированию рынка ИКТ, в том числе и ИБ, под эгидой конференции "ИнфоБЕРЕГ-2014".

— Заменить импортное ПО на написанное "с нуля" российскими программистами во всех сегментах - утопия. Однако есть возможность быстрого рывка к технологической независимости за счет использования открытых свободных технологий, на развитие которых у нас есть все технические возможности и юридические права даже при угрозе самых жестких санкций. Однако само по себе открытое ПО бесполезно без создания локальной инфраструктуры его разработки и наращивания локальной компетенции специалистов. Компания "РОСА" занимается задачей построения такой независимой инфраструктуры и экспертизы с момента основания. Результаты вылились в линейку российских операционных систем, которые могут поддерживаться и развиваться даже в условиях международной изоляции. В своем докладе мы поделились этим опытом и предложили коллегам масштабировать данную модель для обеспечения технологической независимости в других сегментах," - подчеркивает Владимир Рубанов, президент и генеральный конструктор "НТЦ ИТ РОСА".

<<...Центральное место в программе конференции заняли вопросы развития нормативно-правовой базы в сфере ИБ и тема импортозамещения...>>

Большой интерес вызвала секция по безопасности объектов ТЭК, ее ведущим выступил Юрий Иванович Хамчичев, Министерство энергетики РФ. На заседании поднимались проблемы категорирования и паспортизации объектов ТЭК, нормативно-правового регулирования отрасли, а также перспективы развития правовой базы для ТЭК. Для узкого круга специалистов прошла секции по обеспечению транспортной безопасности, некоторые аспекты которой пересекается с безопасностью ТЭК. Представители Минтранспорта и Минэнерго договорились о продолжении диалога на отраслевой конференции "Безопасность критически важных объектов ТЭК", которая состоится в марте 2015г.

Ассоциация электронных торговых площадок (АЭТП) традиционно поддержала конференцию "ИнфоБЕРЕГ". С участием Илии Димитрова, исполнительного директора АЭТП, состоялась горячая экспертная дискуссия по проблемам аутентификации при пользовании электронными госуслугами.

— Мы благодарны участникам конференции "ИнфоБЕРЕГ..Крым" за поддержку и активную работу, - делится впечатлениями Юрий Витальевич Малинин, ректор Академии Информационных Систем, ответственный секретарь Оргкомитета конференции. – Эта конференция стала особенной по ряду причин: мы сменили место проведения, сократили время пребывания и, что приятно, получили одобрение со стороны участников мероприятия. Приятно, что и регуляторы снова выбрали нашу площадку для обсуждения самых острых проблем, а участники – для продвижения общественно значимых идей. Мы надеемся, что все инициативы, о которых говорилось на "ИнфоБЕРЕГ-е" будут реализованы и принесут ощутимый результат всем заинтересованным сторонам.

Генеральный спонсор конференции "ИнфоБЕРЕГ-2014" ГК "Спецпроект", партнеры мероприятия компании "НТЦ ИТ РОСА" и "Диалог Наука". Компания "Ай-Теко" выступит спонсором волейбольного турнира. Генеральный информационный спонсор – Telecom Daily. Организатором мероприятия традиционно выступает Академия Информационных Систем (АИС).

Глава Apple выступил с заявлением о защите личных данных

18 сентября 2014, США
Источник: Total.kz

Тим Кук, Главный исполнительный директор Apple

Главный исполнительный директор Apple Тим Кук (Tim Cook) выступил с заявлением о важности защиты вашей личной информации для Apple.

«Для нас в Apple первоочередное значение имеет Ваше доверие. Именно поэтому мы уважаем Ваше право на конфиденциальность личных данных и защищаем их надежными методами шифрования, а также строгой политикой, которая определяет, как эти данные могут быть использованы», — говорится в заявлении главы Apple, опубликованном в специальном разделе на официальном сайте компании.

По его словам, безопасность и конфиденциальность данных являются важнейшими параметрами, которые учитываются при разработке всех продуктов, программного обеспечения и сервисов, в том числе iCloud и таких новых услуг компании, как Apple Pay. При этом компания не перестает оптимизировать свои продукты.

«Теперь информация о вашей учетной записи Apple ID и все данные, которые Вы храните и обновляете на iCloud, защищены двухэтапной проверкой, к использованию которой мы призываем всех наших клиентов, — подчеркнул Тим Кук. — Мы верим в важность того, чтобы заранее раскрывать Вам всю информацию о том, что будет происходить с персональными данными, которыми Вы делитесь с нами, предварительно запрашивая Ваше разрешение на их получение. Мы также даём возможность легко изменить настройки для ограничения передачи этих данных, если Вы позднее поменяете своё решение. Каждый продукт Apple создан на основе этих принципов. Если мы запрашиваем Ваши данные, то делаем это лишь с целью обеспечить наилучший пользовательский опыт».

Как он отметил, в разделе сайта apple.com/privacy пользователи смогут узнать о том, как Apple обращается с личной информацией клиентов, что именно компания собирает и почему. Здесь же будет появляться (как минимум раз в год или по мере появления значимых изменений политики) вся обновленная информация на тему конфиденциальности личных данных.

«В Apple мы считаем, что отличный пользовательский опыт не должен обеспечиваться за счёт нарушения конфиденциальности данных, — подчеркнул глава компании. — Наша бизнес-модель очень проста: мы продаем продукты. Мы не собираем досье на пользователей на основе содержимого электронной почты или часто просматриваемых веб-страниц для того, чтобы впоследствии продать эту информацию рекламодателям. Мы не "монетизируем" информацию, которую Вы храните на своём iPhone или в iCloud. И мы не читаем Вашу электронную почту или сообщения для того, чтобы получить информацию для продвижения. Наше программное обеспечение и услуги разработаны таким образом, чтобы наши устройства становились всё лучше. Вот и всё».

Тим Кук также пояснил, что лишь одна небольшая часть бизнеса Apple рассчитана на работу с рекламодателями, и это iAd. «Мы создали рекламную сеть, потому как это важно для некоторых разработчиков приложений, и мы хотим поддержать их. Есть и бесплатный сервис iTunes Radio. При этом iAd функционирует в соответствии с той же политикой конфиденциальности, которая применяется и к любым другим продуктам Apple. Сервису недоступны данные приложения "Здоровье" и HomeKit, "Карт", Siri, iMessage, истории звонков и любых других сервисов iCloud, таких как "Контакты" или "Почта", и у Вас всегда есть возможность полностью отказаться от предоставления данных любым приложениям».

В своем заявлении глава Apple заострил внимание на том, что компания никогда не работала ни с одной из государственных структур ни в одной стране над созданием закладок для доступа к данным пользователей в своих продуктах и услугах, равно как и не предоставляла доступа к своим серверам. «И мы никогда не пойдём на это», — заключил Кук.

Утекшие персональные данные в России все чаще используются для «кражи личности»

19 сентября 2014, Россия, Москва
Источник: news.softportal.com

Наталья Касперская, генеральный директор ГК InfoWatch

Аналитический центр компании InfoWatch представил результаты глобального исследования утечек информации за первую половину 2014 г. Впервые в отчет включены не только инциденты, произошедшие по вине внутренних нарушителей, но и утечки, ставшие результатом хакерских атак, сообщили CNews в InfoWatch.

Согласно результатам исследования, Россия удерживает второе место по количеству инцидентов. В исследуемый период было выявлено 96 случаев утечки конфиденциальной информации из российских компаний и государственных организаций. Количество «российских» утечек по сравнению с первым полугодием 2013 г. выросло более чем вдвое.

В мире за первое полугодие 2014 г. было зарегистрировано 654 случая утечки конфиденциальной информации (3,5 инцидента в день), что на 32% превышает аналогичный показатель за прошлый год. Во всем мире скомпрометировано более 450 млн записей, в том числе финансовые и

персональные данные.

Лишь в 22% случаев утечка информации происходила в результате хакерской активности (таргетированной атаки, фишинга, взлома веб-ресурса и пр.). В большинстве случаев (75%) информация утекала по вине внутреннего нарушителя. Однако, как отметили авторы исследования, масштаб последствий не зависит от вектора воздействия — действия и внешних, и внутренних нарушителей могут быть в равной степени разрушительными, привести к компрометации огромных объемов данных.

Доли случайных и умышленных утечек в первом полугодии 2014 г. равны (по 44,6%). Такая картина наблюдается с 2008 г., вследствие чего аналитики делают вывод о стабилизации роста утечек и их распределений, в том числе из-за довольно широкого распространения средств защиты от утечек и контроля информации (впрочем, пока преимущественно в западных странах, на которые приходится более 70% зарегистрированных утечек, указали в InfoWatch).

Что касается утечек, происходивших в результате действий внутренних нарушителей, то в 71% случаев такими нарушителями оказывались рядовые сотрудники компаний — нынешние или бывшие (69,2% и 1,4% соответственно). Велика доля утечек, случившихся на стороне подрядчиков, чей персонал имел легитимный доступ к охраняемой информации (8,4%). При этом в 3,1% случаев ценная информация была скомпрометирована по вине высших руководителей организаций.

В своем отчете InfoWatch впервые приводит классификацию инцидентов по характеру действий нарушителя. К непосредственным утечкам данных относятся 83% случаев компрометации информации, 11% зафиксированных утечек были сопряжены с использованием сотрудниками служебного положения для получения личной выгоды, в 5% утечек произошли вследствие превышения сотрудниками прав доступа к информации.

Если в 2013 г. аналитики говорили о «буме» утечек из государственных органов, то в 2014 г. наблюдались крупные множественные утечки в образовательных и муниципальных учреждениях, госорганах, в высокотехнологичной отрасли (компрометация интернет-сервисов, утечки у провайдеров). Так, были зарегистрированы 14 утечек с числом скомпрометированных записей от миллиона и более. Среди компаний и сервисов, пострадавших от крупных утечек — Experian, Evernote, Snapchat, Orange. В ходе этих 14 крупнейших утечек было скомпрометировано в общей сложности более 430 млн записей клиентов и сотрудников компаний. Утечки чуть меньших объемов данных зафиксированы в медицине, торговле, финансовом секторе.

При этом в организациях среднего размера зафиксировано существенно больше утечек, чем в крупных компаниях, подчеркнули в InfoWatch. В ряде случаев в пределах одной отрасли совокупный объем скомпрометированных записей в средних компаниях равен совокупному объему скомпрометированных записей в крупных компаниях. Все это говорит о том, что вопрос защиты ПДн от утечек для среднего бизнеса сегодня столь же актуален, как и для крупного.

В 38,1% случаев утечка происходила через Сеть (личная электронная почта, облачные хранилища). Доля зарегистрированных утечек через этот канал серьезно выросла по сравнению с прошлым годом — на 17,2 п.п. Львиная доля утечек в первом полугодии 2014 г. пришлась на три основных канала: интернет (38,1%), бумажные документы (17,9%) и кража/потеря оборудования (9,9%). Аналитики считают, что этот рост обусловлен более широким внедрением DLP-систем, работающих в режиме мониторинга, в результате чего компании начали осознавать реальное число происходящих у них инцидентов.

В противоположность утечкам через интернет, зафиксированное число которых можно считать весьма близким к реальному, утечки через мобильные устройства до сих пор находятся «в тени». Формально их доля за исследуемый период составила лишь 0,5%. Однако ввиду практически полного отсутствия контроля за корпоративной информацией, передаваемой через мобильные устройства, можно предположить, что в реальности число подобных инцидентов гораздо выше, считают в InfoWatch.

За исследуемый период подавляющее число случаев компрометации конфиденциальной информации (90,7%) было связано с утечками персональных или платежных данных. Эта тенденция наблюдалась и ранее, но в 2014 г. чуть ли не три четверти утечек персональных данных были так или иначе связаны с «кражей личности». Утекающие данные впоследствии широко использовались в мошеннических схемах (оформление кредитов на чужие данные, фальшивые требования по возврату налогов и проч.).

КОМПЕТЕНТНОЕ МНЕНИЕ:

Наталья Касперская, InfoWatch, генеральный директор

<<Данные 2014 года говорят о том, что российская картина утечек информации все стремительнее приближается к американской. Все большее распространение получает такой вид преступления, как "кража личности" — использование чужих персональных данных в собственных целях. Если раньше мы об этом читали только в иностранных СМИ, сегодня хищение чужих ПДн с целью мошенничества — обычная практика российских преступников. К счастью, для нашей страны пока не характерны массовые атаки на крупные онлайн-сервисы или операторов связи с целью хищения базы данных клиентов. Но это вопрос уже завтрашнего дня. Например, еще пять лет назад кража интеллектуальной собственности у работодателя была экзотикой, а сегодня мы слышим о подобных случаях ежедневно. Поэтому анализ глобальной картины утечек необходим российскому рынку, чтобы отслеживать мировые тенденции и предупреждать те угрозы информационной безопасности, которые возникнут уже завтра.>>

Система Check Point Threat Prevention показала лучшие результаты в сравнительных тестах на обнаружение неизвестных угроз

24 сентября 2014, США
Источник: Пресс-релиз

Check Point® Software Technologies Ltd. (Nasdaq: CHKP), мировой лидер по обеспечению интернет-безопасности, сообщает о том, что система Check Point Threat Prevention достигла результата в 100% по итогам сравнительного тестирования на обнаружение неизвестных угроз. Таким образом, решение Check Point позволяет предоставлять организациям самый высокий уровень защиты от новых целевых атак в интернете.

По итогам недавно проведенного тестирования 300 неизвестных вредоносных файлов были просканированы шлюзами безопасности Check Point 13500, объединенными в систему ThreatCloud™, и несколькими конкурирующими продуктами от трех других поставщиков в области информационной безопасности. Все платформы, участвовавшие в тесте, использовали максимальное количество сервисов предотвращения угроз (IPS, Anti-Malware, Anti-Bot, Threat Emulation) и самый новый набор сигнатур.

Результаты тестирования показали, что Check Point легко обходит конкурирующие решения, обнаруживая 100% неизвестных вредоносных файлов. Система, занявшая второе место, смогла выявить только 70%. В 300 вредоносных файлов входило 40% PDF, 40% EXE и 20% файлов типа DOC.

В ответ на появление все более агрессивных и деструктивных поколений целевых атак, компания Check Point улучшила механизмы обнаружения угроз в своих решениях, предоставив пользователям возможность заранее узнавать о новых, развивающихся угрозах. Глобальное исследование Check Point 2014 Security Report показало, что в среднем организации загружают 53 неизвестных элемента вредоносного ПО в день — по одному каждые 27 минут.

«Хакеры идут все более сложными путями, чтобы выявить и использовать только что обнаруженные уязвимости, вкладывая значительные ресурсы в разработку новых вариантов вредоносного ПО и формируя новые векторы атаки для проникновения в сеть. По данным нашего исследования, с 2012 года количество атак нулевого дня увеличилось на 144%, и это показывает, насколько часто организации сталкиваются со сложными и неизвестными угрозами, — говорит Габи Рейш (Gabi Reish), вице-президент по управлению продуктами Check Point Software Technologies. — Обнаруживая 100% неизвестных вредоносных файлов, наши технологии Threat Prevention обеспечивают заказчикам самый высокий уровень защиты от еще не изученного вредоносного ПО в рамках самой полной многоуровневой системы защиты».

Являясь частью системы предотвращения угроз Check Point's Threat Prevention, решение Threat Emulation обнаруживает и предотвращает заражение от неизученных эксплойтов, неизвестных вариантов вредоносного ПО, а также предотвращает целевые атаки благодаря динамической эмуляции работы файлов в «песочнице». Threat Emulation обеспечивает быстрое обновление средств безопасности и блокирует новейшие атаки в реальном времени, в то время как конкурирующие системы других производителей обнаруживают неизвестное вредоносное ПО, но не могут предотвратить его попадание в сеть. Они позволяют всем файлам проникать внутрь периметра, допуская загрузку и запуск подозрительных файлов. В результате новые сигнатуры, позволяющие блокировать неизвестные вредоносные файлы, создаются с задержкой в 30 минут или более. Эта задержка создает достаточный интервал для того, чтобы вредоносное ПО заразило сеть.

Сразу после обнаружения исследователи Check Point немедленно оценивают принципы поведения и параметры неизвестных угроз и быстро разрабатывают защиту от них. Данные автоматически рассылаются на все шлюзы Check Point, объединенные в глобальный сервис ThreatCloud™. ThreatCloud™ — это коллективная интеллектуальная сеть изучения угроз Check Point, которая обеспечивает защиту для заказчиков компании по всему миру. Во время теста «Unknown 300», решение Check Point стало единственным, которое показало возможность одновременного обнаружения и предотвращения угроз, при том, что конкуренты смогли только обнаружить новые угрозы и атаки.

По данным о перемещениях можно установить личность

30 сентября 2014, Сингапур
Источник: rosinvest.com

Геолокационные сервисы небезопасны, если вы печетесь о своей анонимности: к такому выводу пришла группа сингапурских ученых. Современные технологии позволяют вычислить сферу интересов и точки присутствия почти любого человека.

Исследовательская группа, частично финансируемая Советом экономического развития и Национальным исследовательским фондом Сингапура, выяснила, что удаление или подмена персональных идентификаторов в базах провайдеров не обеспечивает анонимности. При накоплении некоторого объема данных о перемещениях конкретного человека его можно идентифицировать по траектории этих перемещений. Причем, чем длиннее траектория и чем чаще она воспроизводится, тем проще это сделать.

«Not So Unique in the Crowd: a Simple and Effective Algorithm for Anonymizing Location Data» — исследование мобильных данных порядка 630 тыс. пользователей, собранных за неделю. Несмотря на

то, что местоположение пользователей слегка размыто, и, по сути, представляет собой данные о местоположении оборудования, более 60% траекторий в базе оказались уникальными.

Авторы предлагают простой метод снижения уникальности траекторий передвижения пользователя путем разбивки ее на суб-траектории и снижения периода фиксации информации, например, до 6 часов. Этот подход позволяет снизить уникальность траекторий до 30% и при этом сохранить информативность базы данных, что немаловажно для последующих аналитических целей и предоставления пользователю качественного сервиса. Однако полностью проблему анонимности владельца мобильного устройства это не решает.

Владимир Уфнаровский, исполнительный директор компании «Ланит-Терком»

Существуют ли в принципе анонимизированные данные, объясняет Юрий Наместников, антивирусный эксперт «Лаборатории Касперского»: «Существуют методы анонимизации и защиты данных, но они требуют минимальной технической подготовки от человека. Например, можно использовать системы шифрования, защищенное соединение (к примеру, VPN) и другие системы анонимного доступа в сеть. Но в первую очередь, пользователь сам должен захотеть уменьшить свой цифровой след — по возможности, отключать сервисы сбора статистики и геолокации».

Сложность извлечения ценной информации из подобных данных, зависит, по мнению эксперта, от того, насколько хорошо информация анонимизирована самим сервисом, который собирает данные, и от системы защиты этого сервиса.

Олег Юдин, руководитель отдела маркетинга компании Artezio отмечает, что любая информация при обмене данными доступна специалистам компании, предоставляющей сервис. «Если вы хотите анонимизированного использования GPS, пользуйтесь им только как приемником сигнала спутников и определения местоположения на заранее загруженных картах. А вообще для мобильных технологий анонимность пользователей и защита персональных данных только начинает развиваться. В качестве примера можно привести Android-приложение Orbot на основе так называемой «луковой» маршрутизации (Tor), где анонимность обмена информацией достигается за счет использования системы прокси-серверов, через которые данные передаются в зашифрованном виде».

Владимир Уфнаровский, исполнительный директор компании «Ланит-Терком», считает, что любой человек, носящий смартфон, автоматически соглашается на то, что, при желании, о нем можно собрать любые данные. «При наличии огромного количества личной информации, которую люди совершенно добровольно сообщают о себе в социальных сетях, Twitter и др., совершенно необязательно беспокоиться о каком-либо «нарушении анонимности» при анализе траекторий передвижений, которые потенциально может выполнить какой-нибудь специалист».

С коллегами согласен и Дмитрий Дудко, руководитель проектов по информационной безопасности Центра компетенции информационной безопасности «АйТи»: «Я не разделяю идею того, что какая-то информация в принципе может быть анонимной. Любые действия и данные оставляют след, вопрос лишь в желании и возможности эти следы найти и составить из них цепочку до источника».

«Доктор Веб» подготовил обзор мобильных угроз за сентябрь 2014

02 октября 2014, Россия, Москва
Источник: securrity.ru

Как и в предыдущие месяцы, в сентябре специалисты компании «Доктор Веб» зафиксировали многочисленные атаки на мобильные устройства пользователей. В частности, вирусная база Dr.Web пополнилась множеством новых записей для распространяемых злоумышленниками Android-угроз, среди которых были банковские трояны, трояны-вымогатели, вредоносные программы-шпионы и даже опасный троян-вандал. Также в вирусную базу была внесена очередная запись для вредоносного приложения, работающего на «взломанных» мобильных устройствах производства компании Apple, сообщили CNews в «Доктор Веб».

В сентябре специалисты компании зафиксировали появление новых представителей банковских троянов, предназначенных для получения незаконного доступа к счетам пользователей. Многие из обнаруженных «банковских» угроз предназначались для владельцев Android-смартфонов и планшетов, принадлежащих жителям Южной Кореи. Традиционно большинство банковских Android-троянов, циркулирующих в этой стране, распространяется злоумышленниками при помощи нежелательных SMS-сообщений, содержащих ссылку на загрузку вредоносного приложения. В прошлом месяце было зафиксировано более 100 подобных спам-кампаний, при этом среди наиболее распространенных угроз оказались трояны Android.Banker.28.origin (22,64%), Android.BankBot.27.origin (21,70%), Android.SmsSpy.78.origin (14,15%), Android.SmsBot.121.origin (11,32%), Android.MulDrop.21.origin (9,43%) и Android.Banker.32.origin (7,55%).

Не остаются в стороне от атак злоумышленников и пользователи из Поднебесной. Среди исследованных в сентябре Android-угроз оказался и очередной троян-шпион, крадущий конфиденциальную информацию у китайских владельцев мобильных устройств. Эта вредоносная программа, получившая по классификации «Доктор Веб» имя Android.Spy.130.origin, опасна тем, что передает контролирующим ее злоумышленникам сведения об SMS-переписке, совершенных звонках, текущих GPS-координатах, а также способна незаметно выполнить звонок на заданный номер, превращая зараженный смартфон или планшет в прослушивающее устройство.

В тренде по-прежнему находятся трояны, блокирующие мобильные Android-устройства и требующие деньги за их разблокировку, количество этих вымогателей продолжает расти. Среди обнаруженных в прошлом месяце подобных угроз наибольший интерес представляет троян Android.Locker.38.origin, который, помимо блокировки экрана сообщением с требованием оплаты выкупа, обзавелся дополнительным инструментом по выманиванию денег у пользователей. Как и его собратья, эта вредоносная программа устанавливается в систему под видом безобидного приложения (в данном случае — якобы системного обновления) и после запуска запрашивает доступ к правам администратора мобильного устройства. Далее Android.Locker.38.origin блокирует его и требует оплату за разблокировку.

При попытке пользователя отозвать у трояна предоставленные ему полномочия вредоносная программа блокирует экран стандартной системной функцией и после его разблокировки угрожает владельцу зараженного Android-смартфона или планшета удалением всей хранящейся на устройстве информации. Если пользователь проигнорирует эту угрозу и отзовет права администратора, Android.Locker.38.origin установит на разблокировку мобильного устройства из режима ожидания собственный пароль, в результате чего для дальнейшей работы может потребоваться сброс всех настроек.

<<...В тренде по-прежнему находятся трояны, блокирующие мобильные Android-устройства и требующие деньги за их разблокировку, количество этих вымогателей продолжает расти...>>

Весьма необычной на фоне прочих Android-троянов оказалась вредоносная программа Android.Elite.1.origin, которая не предназначалась для извлечения прибыли киберпреступниками. Тем не менее, данная мобильная угроза все же представляла существенную опасность для владельцев Android-устройств. Будучи запущенным на зараженном смартфоне или планшете, Android.Elite.1.origin выполнял форматирование карты памяти, удаляя с нее всю информацию, а также блокировал работу ряда приложений для онлайн-общения и SMS-переписки. Кроме того, этот троян производил массовую рассылку SMS-сообщений по всем контактам, сохраненным в телефонной книге пользователя, что могло послужить чрезвычайно быстрому опустошению счета мобильного телефона.

Не забывают киберпреступники и о других мобильных платформах, таких как операционная система iOS от Apple. В сентябре в вирусную базу «Доктор Веб» была внесена запись для одного из компонентов трояна IPhoneOS.PWS.Stealer.2, заражающего мобильные устройства под управлением iOS, которые были подвержены «взлому» самими пользователями с целью расширения их функционала (так называемый jailbreak). Данный троян, известный с весны текущего года, похищает аутентификационные данные, такие как логины и пароли, которые необходимы для покупки приложений в магазине App Store, в результате чего злоумышленники могут совершать в нем покупки от имени своих жертв, опустошая их карман.

R-Style представила на InfoSecurity решения по обеспечению безопасности бизнес-систем

03 октября 2014, Россия, Москва
Источник: Пресс-релиз

Системный интегратор R-Style принял участие в Infosecurity Russia 2014. Компания представила на мероприятии, состоявшемся 24-26 сентября в «Крокус-Экспо», решения по обеспечению безопасности бизнес-систем. Тема «Безопасности бизнес-систем» нашла подтверждение в оформлении стенда компании, а также в выступлениях экспертов в деловой части мероприятия.

В рамках деловой программы ключевые эксперты Центра информационной безопасности R-Style – Евгений Акимов, Олег Глебов и Даниил Казаков – представили свой взгляд на наиболее актуальные вопросы обеспечения ИБ, которые интересуют современные компании:

- Как можно совместить интересы ИТ и бизнеса при внедрении IdM, Даниил Казаков

- Как обеспечить экономическую безопасность: выявить неблагонадежных контрагентов и недобросовестных сотрудников, Олег Глебов

- Как на смену эре инфраструктурной безопасности пришла эра интеллектуальной, Евгений Акимов

На стенде R-Style у каждого посетителя была возможность посмотреть демонстрацию этих и других решений по обеспечению безопасности бизнес-систем и получить консультацию эксперта.

Современный подход компании к вопросу обеспечения безопасности бизнес-систем организации вызвал живой интерес как у специалистов компаний разных отраслей бизнеса, так и у представителей СМИ. Большое внимание аудитории к решениям компании R-Style продемонстрировало актуальность выбранной стратегии, а также потребность рынка в подобных предложениях.

«В своем участии в Infosecurity Russia 2014 мы сделали упор на экспертные доклады, затрагивающие самые злободневные тематики – от повышения отдачи от наиболее ресурсоёмких проектов по ИБ до противодействия мошенничеству, – говорит Евгений Акимов, директор Центра информационной безопасности R-Style. – Обозначенные в докладах тематики мы подкрепили демонстрацией на стенде конкретных решений: IdM, DLP, AntiFraud, WAF, – что позволило, не увлекаясь теорией, перейти непосредственно к практике и показать работу той или иной передовой технологии».

R-Style – крупнейший поставщик ИТ-решений и бизнес-систем. Компания 23 года успешно работает на высокотехнологичном рынке России и стран СНГ.

R-Style специализируется на реализации комплексных проектов «под ключ» и поддерживает высокие компетенции в области инфраструктуры, информационной безопасности, телекоммуникации и связи, разработки и внедрении бизнес-решений, специализированного (заказного) ПО, инженерных систем, ИТ-аутсорсинга, ИТ-консалтинга, а также обучения в сфере ИТ.

Среди заказчиков компании R-Style: Пенсионный фонд России, Центральный Банк России,

Федеральная налоговая служба России, Федеральное казначейство, Федеральная служба охраны,

ОАО «Электронная Москва», ОАО «Российские железные дороги», ФГУ «Росгранстрой», ДИТ города Москвы, ФСФР России, Министерство юстиции России, Сбербанк России, Райффайзен Банк, ОАО «Аэрофлот», Ростелеком, ОАО «МТС», Вымпелком (Билайн), ОАО «Мегафон», Большой Театр, Knauf, СИБУР, Красный Квадрат, Евровидение, Oriflame, Очаково, Вимм-Билль-Данн, Русснефть, ФСК, РусГидро и многие другие.

В Москве состоялась 11-я Международная выставка InfoSecurity Russia‘2014

03 октября 2014, Россия, Москва
Источник: infosecurityrussia.ru

С приветственными словами на торжественной церемонии открытия выступили: Шерстюк Владислав Петрович – Советник секретаря СБ РФ, Директор Института проблем информационной безопасности МГУ им. М.В.Ломоносова, Куц Анатолий Владимирович – Заместитель директора ФСТЭК России, Мурашов Николай Николаевич – заместитель начальника Центра ФСБ России, Крылов Олег Вячеславович – начальник ГУБЗИ Банка России, Мирошников Борис Николаевич – член экспертного совета, руководитель комитета по информационной безопасности НП "Национальный платежный совет", Емельянов Геннадий Васильевич – Президент МОО "АЗИ", Шаклеин Дмитрий Иванович – член Экспертного совета комитета по безопасности и противодействию коррупции Государственной Думы ФС РФ, Вараксин Владимир Алексеевич – первый заместитель Генерального директора, "Гротек", Рохмистрова Наталья Борисовна – Директор выставки InfoSecurity Russia / ItSec by Groteck, "Гротек".

25 сентября выставку посетил Директор ФСТЭК России Владимир Викторович Селин.

Владимир Викторович Селин с делегацией осмотрел экспозицию выставки и ознакомился с решениями ведущих российских и зарубежных производителей.

25 сентября заместитель мэра Москвы в Правительстве Москвы по антитеррористической деятельности Виктор Николаевич Захаров посетил InfoSecurity Russia‘2014 / ItSec by Groteck.

Виктор Николаевич Захаров, заместитель мэра Москвы в Правительстве Москвы по антитеррористической деятельности:

"Посещение выставки обусловлено тем, что на этой авторитетной и представительной площадке имеется возможность ознакомиться с современными разработками и подходами к решению вопросов обеспечения информационной безопасности как объектов ТЭК, так и в целом автоматизированных систем управления технологическими процессами, технологиями противодействия угрозам кибертерроризма".

Деловая программа InfoSecurity Russia‘2014 / ItSec by Groteck осветила самые актуальные темы, которые наиболее интересны сообществу специалистов и заказчиков рынка информационной безопасности. В течение трех дней в шести конференц-залах выставки в режиме нон-стоп проходили конференции, круглые столы, пленарные заседания, обучающие семинары. Среди главных тем: защита АСУ ТП, импортозамещение, противодействие мошенничеству, защита персональных данных, облачные технологии, DLP, безопасность электронных платежей, защита онлайн-банка, экономическая безопасность, межсетевые экраны нового поколения и др. Традиционно в деловой программе приняли участие признанные эксперты рынка информационной безопасности России и авторитетные международные спикеры.

Михаил Емельянников, Управляющий партнер "Емельянников, Попова и партнеры":

"Я считаю, что аналога этой выставки в России нет, это единственная отраслевая выставка с мощной деловой программой. Просто конференции, которые проходят и два, и три дня, не заменяют это мероприятие, потому что кроме конференции здесь есть возможность увидеть, попробовать, потрогать руками, поговорить со специалистами, а не только выслушать доклад одного маркетолога. Организаторы должны прилагать все усилия, чтобы она и дальше росла и развивалась".

Экспозиция выставки выросла на 21%.

Каждый посетитель смог получить подробную информацию о продуктах в области мобильной безопасности, облачных решений, защиты ПДн, сетевых решений, криптографии, антивирусов, центров хранения данных, ЭДО, удостоверяющих центров, электронной защиты периметра, электронных госуслуг, виртуализации, управления идентификацией и многих других.

Количество участников InfoSecurity Russia‘2014/ItSec by Groteck пополнилось ведущими российскими и зарубежными компаниями, такими как: "Лаборатория Касперского", "Информзащита", "Энвижн Груп", НПО РусБИТех, НОВ GmbH & Co. KG, Thales e-Security , Juniper Networks, Nexetic и многими другими.

Кроме того, в соответствии с запросами заказчиков было организовано четыре тематические демо-зоны.

Внимание регуляторов и государственных заказчиков привлекла новая демо-зона "Сделано в России", где посетители смогли ознакомиться с передовыми технологиями отечественных производителей.

<<...В этом году предварительная регистрация на выставку выросла на 39% по сравнению с прошлым годом и достигла цифры 8312 человек...>>

В демо-зоне "Инновации Сколково" компании-резиденты IT-центра "Сколково", специализирующиеся в сфере информационной безопасности, представили свои новейшие технологические решения и разработки.

Сергей Ходаков, руководитель направления "Безопасные информационные технологии" ИТ-кластера Фонда "Сколково":

"Мы уверены, что участие в Infosecurity Russia’2014/ItSec by Groteck придаст новый импульс развитию наших проектов, которые были на нем представлены".

В демо-зоне "Межсетевые экраны" посетители могли ознакомиться с экранами нового поколения и по заданному набору критериев выбрать подходящий МсЭ для своей компании.

В демо-зоне "Экономическая безопасность" были представлены решения по криминалистике, защите коммерческой тайны, кадровой безопасности.

В этом году предварительная регистрация на выставку выросла на 39% по сравнению с прошлым годом и достигла цифры 8312 человек. Количество предварительно назначенных встреч побило рекорд прошлого года, превысив цифру 18000.

По предварительной оценке общее количество посетителей выставки выросло на 7% по сравнению с прошлым годом.

Виктор Сердюк, Генеральный директор "Диалог Наука":

"Компания Диалог Наука является постоянным участником выставки InfoSecurity Russia/ItSec by Groteck. Для нас это-хорошая площадка, чтобы представить свои новые продукты, услуги, пообщаться с существующими заказчиками и найти новые контакты заказчиков, с которыми мы еще не работали".

Комфортная обстановка на площадке позволила поставщикам и покупателям продуктивно работать все три дня. Переговоры и обучение шли нон-стоп в экспозиции, демо-зонах, на мероприятиях, в ресторанах и зонах отдыха. Атмосферу праздника помогли создать интерактивные игры: "Нарасти IT-карму", "Колесо фортуны" с NFC-технологиями и программа PassPort-game.

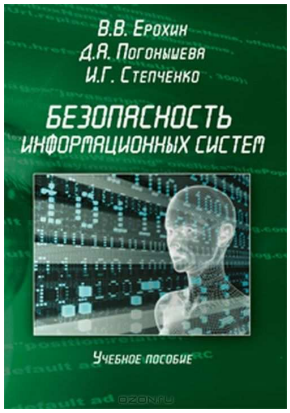
Андрей Мирошкин, Генеральный директор "Гротек":

"В этом году можно смело сказать, что InfoSecurity Russia’2014/ItSec by Groteck достигла нового уровня организации. Это стало результатом совместной работы организаторов, партнеров, экспонентов и экспертов отрасли, которые вносят свои идеи и участвуют в их реализации при подготовке и проведении мероприятия. Это делает выставку профессиональным событием, удовлетворяющим интересы сообщества. Будем применять эти принципы и в дальнейшем для развития и роста InfoSecurity Russia / ItSec by Groteck!"

АНОНСЫ

Новинки профессиональной литературы

Безопасность информационных систем



Автор: Ерохин В.В, Погонышева Д.А., Степченко И.Г.
Год: 2015
Источник: ozon.ru

В пособии излагаются основные тенденции развития организационного обеспечения безопасности информационных систем, а также подходы к анализу информационной инфраструктуры организационных систем и решению задач обеспечения безопасности компьютерных систем. Для студентов по направлению подготовки 230400 — Информационные системы и технологии (квалификация «бакалавр»).

Издание 1-е.

Основы организационно-правовой защиты информации

Автор: Борисов Михаил, Романов Олег
Издательство: Ленанд
Год: 2015
Источник: ozon.ru

В настоящем пособии изложены вопросы организационно-правовой оценки защиты информации в органах государственной власти, на предприятиях различных форм собственности, в коммерческих организациях и учреждениях. Рассмотрено понятие конфиденциальности информации, изложены принципы и критерии отнесения информации к коммерческой тайне, вопросы организации допуска и доступа персонала к конфиденциальной информации; описываются основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации, организация защиты информации при проведении совещаний и в ходе издательской и рекламной деятельности. Освещаются вопросы организации аналитической работы и контроля состояния защиты конфиденциальной информации.

Учебное пособие предназначено для студентов, обучающихся по специальностям "Математические методы и программное обеспечение защиты информации", "Информационная безопасность", "Защита информационных технологий", "Обеспечение защиты информации в автоматизированных системах военного назначения". Рекомендуется для изучения руководителям и специалистам по информационным технологиям и защите информации коммерческих структур.

4-е издание.

Технические, организационные и кадровые аспекты управления информационной безопасностью

Автор: Милославская Наталья, Сенаторов Михаил, Толстой Александр
Издательство: Горячая Линия - Телеком
Год: 2014
Источник: ozon.ru

Рассмотрены технические аспекты управления информационной безопасностью (ИБ), включая управление логическим доступом пользо-вателей к активам организации, управление защищенной передачей дан-ных и операционной деятельностью, разработку и обслуживание инфор-мационных систем с учетом требований к их ИБ, управление конфигура-циями, изменениями и обновлениями в активах организации. Кратко рас-смотрены основы физической защиты и защиты от воздействия окру-жающей среды. Анализируются организационные и кадровые вопросы управления ИБ. Введены четыре основные модели организационного управления ИБ, яв-

ляющиеся комбинациями централизованных и децен-трализованных руководства и администрирования ИБ. Рассмотрена ор-ганизационная инфраструктура управления ИБ. Перечислены организа-ционные мероприятия по управлению ИБ. Подробно описаны деятель-ность, функции, состав и варианты создания службы ИБ организации, а также задачи, функции, обязанности, права и ответственность администт-ратора ИБ подразделения организации. Детально анализируются группы компетенций, должности и направления деятельности специалистов в области ИБ. Особое внимание уделено учету вопросов ИБ при найме персонала на работу и при формировании должностных обязанностях персонала.

Для студентов вузов, обучающихся по программам бакалавриата и магистратуры направления 090900 - ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, будет полезно слушателям курсов переподготовки и повышения квали-фикации и специалистам.

2-е издание, исправленное.

Обучение / повышение квалификации

Семинар «Что такое аудит информационной безопасности и как правильно его провести?»

Период работы: 05.12.2014 - 05.12.2014
Место проведения: Россия, Москва
Организатор - ЗАО «ДиалогНаука»,
+7(495)980-67-76, +7(499)670-95-95
Источник: dialognauka.ru

Современные автоматизированные системы играют важную роль в обеспечении эффективного выполнения бизнес-процессов предприятий и организаций. Повсеместное использование систем для хранения, обработки и передачи информации приводит к повышению актуальности проблем, связанных с их защитой.

Для того чтобы гарантировать эффективную защиту от информационных атак злоумышленников, компаниям сегодня необходимо иметь объективную и независимую оценку текущего уровня безопасности автоматизированных систем. Именно для этих целей и применяется аудит информационной безопасности, практические аспекты проведения которого будут рассмотрены в рамках семинара.

Участники семинара ознакомятся с различными видами аудита безопасности, методиками и практическими особенностями его проведения для различных типов автоматизированных систем.

Программа семинара:

Секция №1 (Виктор Сердюк, генеральный директор ЗАО «ДиалогНаука»):

Что такое аудит информационной безопасности? Как можно провести аудит информационной безопасности? Основные этапы работ по проведению аудита безопасности. Методы сбора и анализа исходной информации для проведения аудита. Результаты проведения аудита. Возможности системы RedSeal Networks для проведения аудита безопасности.

Секция №2 (Роман Ванерке, Руководитель отдела технических решений ЗАО «ДиалогНаука»):

Инструментальный аудит и оценка соответствия стандартов с помощью ПО MaxPatrol.

Секция №3 (Андрей Соколов, консультант по информационной безопасности ЗАО «ДиалогНаука»)

Особенности проведения теста на проникновения из сети Интернет.

Секция №4 (Андрей Масалович, руководитель направления конкурентной разведки ЗАО «ДиалогНаука»):

Аудит утечек конфиденциальной информации на основе технологий конкурентной разведки

Вебинар «Использование решения agileSI для мониторинга информационной безопасности систем SAP»

Период работы: 02.12.2014 - 02.12.2014
Место проведения: Россия, Москва
Организатор - ЗАО «ДиалогНаука»,
+7(495)980-67-76, +7(499)670-95-95
Источник: dialognauka.ru

Программное обеспечение agileSI, предназначено для мониторинга информационной безопасности ERP-систем SAP.

agileSI обеспечивает: постоянный анализ SAP систем на предмет наличия эксплуатационных уязвимостей, ошибок в конфигурации, превышения полномочий, а также может использоваться для мониторинга критических транзакций и действий пользователей; автоматизацию процесса сбора, корреляции и визуализации информации о событиях безопасности; формирование отчетов о текущем состоянии ин-

формационной безопасности системы SAP; снижение затрат на аудит информационной безопасности SAP; обнаружение атак на системы SAP; возможность обрабатывать события безопасности систем SAP в рамках единого ситуационного центра информационной безопасности.

Результаты работы системы agileSI могут передаваться для дальнейшей обработки в такие SIEM-решения как HP ArcSight, IBM QRadar, Splunk, Logpoint или LogRhythm.

Спикер: Николай Петров, CISSP, Директор по развитию бизнеса, ЗАО «ДиалогНаука»

Программа вебинара:

- Важность мониторинга SAP и примеры уязвимостей;

- Обзор решения agileSI;

- Сравнение с другими решениями;

- Ответы на вопросы.

ППК-4ТЗ: «Организация технической защиты конфиденциальной информации»

Период работы: 02.02.2015 - 13.02.2015
Место проведения: Россия, Санкт-Петербург
Организатор - НОУ ДПО «Центр предпринимательских рисков, +7(812)234-95-48, +7(812)234-95-65, +7(812)234-95-66, +7(812)346-48-93
Источник: cprspb.ru

Программа повышения квалификации предназначена для: руководителей предприятий и организаций различных форм собственности, руководителей, начальников отделов (служб, групп и т.д.), ведущих (главных) специалистов и специалистов подразделений безопасности (информационной безопасности), руководителей и сотрудников специализированных подразделений по защите конфиденциальной информации и по противодействию экономическому шпионажу, руководителей и сотрудников отделов автоматизации, вычислительных центров, информационно-технических отделов.

Целевая установка: обучение на данном курсе является обязательным при получении предприятием лицензии на право проведения работ по защите конфиденциальной информации; программа обучения согласована с ФСТЭК России и рассматривает правовые, организационные и технические аспекты создания и функционирования системы защиты информации ограниченного доступа.

Содержание программы:

введение в курс; угрозы безопасности конфиденциальной информации (каналы утечки конфиденциальной информации, состояние и перспективы развития технических средств добывания конфиденциальной информации); основы защиты конфиденциальной информации (правовые основы защиты конфиденциальной информации, государственная система защиты информации, нормативно-методические документы ФСТЭК РФ по защите информации, методология обеспечения защиты конфиденциальной информации); организация и обеспечение работ по технической защите конфиденциальной информации (основы организации работ по защите конфиденциальной информации, основы обеспечения защиты конфиденциальной информации, специальные требования и рекомендации по защите конфиденциальной информации); средства технической защиты конфиденциальной информации (средства защиты от несанкционированного физического доступа на объекты информатизации, средства защиты конфиденциальной информации в автоматизированных системах, средства защиты конфиденциальной информации от утечки за счет ПЭМИН, средства защиты конфиденциальной информации от утечки по акустическому, виброакустическому и оптическому каналам); контроль защищенности конфиденциальной информации (организация контроля защищенности конфиденциальной информации, техническое обеспечение контроля защищенности конфиденциальной информации, порядок проведения контроля защищенности конфиденциальной информации).

Деловой календарь

Конференция "Защита персональных данных: исполнение и наказание"

Период работы: 09.12.2014 - 09.12.2014
Место проведения: Россия, Москва
Организатор - CNews Conferences,
+7(495)363-11-11 доб. 3141, 3477, 3435, 3439
Источник: events.cnews.ru

Внесенные в июле 2011 года изменения в ФЗ-152 «О персональных данных», который был принят еще в 2006 году и неизменно вызывал нарекания со стороны участников рынка, казалось бы, более четко определили регламенты взаимоотношения личности, общества и государства. «Вторая редакция» закона расширила круг обязанностей операторов ПДн: помимо технической защиты информации, теперь должен быть обеспечен и целый комплекс организационно-правовых мероприятий. Тем, кто нарушил данное предписание, грозят реальные штрафы.

Однако исполнить в полном объеме 152-ФЗ предприятиям непросто по целому ряду причин как технического, так и организационного характера. К тому же, как отмечают эксперты, еще не завершен процесс создания вокруг закона необходимой системы подзаконных актов. Есть даже мнение, что выполнение требований позволит лишь создать видимость безопасности, но отнюдь не гарантировать реальную защищенность персональных данных коммерческих и государственных предприятий.

Вопросы конференции:

- В какой степени ФЗ-152 «О персональных данных» соответствует требованиям международного права?

- В чем принципиальное отличие российского варианта закона о защите ПДн от мировых?

- Каких новых инициатив ждать от регуляторов?

- Чем рискует оператор ПДн, игнорирующий требования законодательства?

- В какой степени реально защищен российский клиент, доверивший персональные данные предприятию?

- С чего начать внедрение комплекса мер по обеспечению защиты ПДн?

- Эффективно ли, что в России наказывают не за утечку данных о клиенте, а за несоответствие требованиям?

- Каков должен быть размер штрафа за несоблюдение требований по защите ПДн, чтобы квалифицироваться как бизнес-значимый?

- Есть ли пропасть между реальной защищенностью ПДн и той, которую могут обеспечить выполнение требований регуляторов?

Межрегиональная специализированная выставка "Связь. Транспорт. Безопасность - 2014"

Период работы: 11.11.2014 - 13.11.2014
Место проведения: Россия, Якутск
Организатор - ООО "СибЭкспоСервис",
+7(383)335-63-50
Источник: ses.net.ru

Место проведения: Дворец спорта "50 лет Победы".

Основные тематические разделы:

- Связь: средства и системы всех видов связи, телекоммуникации, услуги операторов связи, салоны связи, сервисные центры; локальные, корпоративные и глобальные сети (оборудование, технологии); интернет (услуги провайдеров, веб-хостинг, создание и поддержка веб-сервисов, веб-дизайн); телевидение, мультимедиа, спутниковые технологии.

- Транспорт: спецтехника, промышленная техника, специальный транспорт, городской транспорт; транспортные, логистические услуги; альтернативные источники энергии на транспорте; строительство дорог, мостов, тоннелей, инновационные технологии на транспорте и в промышленности; мониторинг, системы охраны, слежения, оповещения, видеонаблюдения, связи, сигнализации на транспорте, контроль топлива; страхование транспорта и транспортных услуг.

- Безопасность: системы охраны, контроля доступа, слежения, навигации, оповещения, видеонаблюдения, связи, сигнализации; пожарная безопасность; безопасность на гражданских и промышленных объектах, охрана труда; антитеррористическое и досмотровое оборудование; информационная безопасность, персональные данные, системы защиты баз данных; безопасность на всех видах транспорта: охрана и сопровождение грузовых и пассажирских перевозок; страхование: жизни, имущества, оборудования, транспорта, промышленных объектов.

Межрегиональная специализированная выставка "Безопасность - 2014"

Период работы: 25.11.2014 - 27.11.2014
Место проведения: Россия , Екатеринбург
Организатор - "Уральские выставки",
+7(343)385-35-35
Источник: uv66.ru

Основные тематические разделы:

- Пожарная безопасность: системы пожарной сигнализации и оповещения; системы и средства пожаротушения; огнезащитные материалы и конструкции; экипировка и снаряжение; пожарная техника и специальные агрегаты; средства эвакуации и спасения при пожарах.

- Системы охраны: системы охранного телевидения и наблюдения; системы контроля доступа; системы охранной сигнализации.

- Средства спасения: техника, технологии, оборудование для предотвращения аварий, катастроф и ликвидации их последствий; оборудование для оказания первой помощи; спасательные устройства; экипировка и снаряжение спасателей; средства жизнеобеспечения; средства индивидуальной защиты; средства связи и оповещения.

- Экологическая и промышленная безопасность.

- Безопасность дорожного движения: средства организации дорожного движения; системы обеспечения безопасности водителя и пассажиров; средства контроля и надзора за безопасностью дорожного движения.

- Банковская безопасность: специальное банковское оборудование; услуги инкассации; спецтранспорт.

- Безопасность и охрана труда: организация труда; средства индивидуальной защиты; услуги по аттестации рабочих мест; обучение специалистов по охране труда; научно-исследовательские организации, институты, ассоциации; специализированная литература; программное обеспечение.

- Безопасность информации и связи: защита информации и средства автоматического засекречивания связи; технические средства поиска каналов утечки информации; информационная безопасность; биометрические системы защиты информации; обучение, услуги в области консалтинга и аудита информационной безопасности.

- Специальная одежда: профессиональная одежда; ведомственная одежда; корпоративная одежда; корпоративная одежда для различных отраслей; специальная обувь; экипировка и вспомогательное оборудование.

- Антикриминал: специальный полицейский транспорт; экипировка, обмундирование, боевое снаряжение; специальная техника и аппаратура для скрытого наблюдения, прослушивания, записи съёмки; аппаратура для обнаружения подслушивающих устройств; оборудование, техника, приборы, реактивы для криминалистики; специальный транспорт для перевозки ценностей; хранилища, защитные кабины, сейфы, специальная тара для переноски ценностей; контрольно-пропускные пункты, турникеты, шлагбаумы, механизированные ворота; системы санкционированного доступа; технические средства досмотра людей и грузов; технические средства обнаружения наркотиков, скрытых взрывных устройств; услуги частных охранных и сыскных агенств.

ИСТОРИЧЕСКИЙ РАКУРС: ОКТЯБРЬ

01 октября 2008 (6 лет назад)

Россия ратифицировала Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации

Россия, Москва
Источник: garant.ru

Эмблема СНГ

Федеральным законом от 1 октября 2008 N 164-ФЗ Россия ратифицировала Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации. Соглашение было подписано в Минске 1 июня 2001. Целесообразность ратификации Соглашения обусловлена потребностью в расширении правовых основ сотрудничества правоохранительных и судебных органов государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации.

Соглашением определяются ключевые направления и формы сотрудничества в области борьбы с преступлениями в сфере компьютерной информации (обмен информацией, основания и порядок исполнения за-

просов об оказании содействия), а также перечень уголовно наказуемых деяний.

ФЗ предусматривается возможность отказа в исполнении запроса об оказании содействия полностью или частично только в случае, если запрашиваемая Сторона полагает, что его исполнение противоречит ее национальному законодательству. При этом Уголовно-процессуальным кодексом РФ установлено, что запрос возвращается без исполнения, если он противоречит законодательству РФ либо его исполнение может нанести ущерб ее суверенитету или безопасности.

Компетентными органами в рамках Соглашения являются МВД России, ФСБ России, Генеральная прокуратура РФ, Мининформсвязи России.

04 октября 1965 (49 лет назад)

Родился Евгений Валентинович Касперский - российский программист, один из ведущих мировых специалистов в сфере информационной безопасности

Россия, Краснодарский край
Источник: kalendar.it.ru

Евгений Валентинович Касперский

4 октября 1965, Новороссийск

Один из основателей, основной владелец и нынешний глава ЗАО «Лаборатория Касперского» — международной компании, занимающейся разработкой решений для обеспечения IT-безопасности, имеющей более 30 региональных офисов и ведущей продажи в 200 странах. Лауреат Государственной премии в области науки и технологий за 2008 год. В прессе характеризуется как «гроза компьютерной преступности».

Еще в школе Касперский начал углубленное изучение математики в рамках спецкурса. После победы в математической олимпиаде в 1980 был зачислен в физико-математическую школу, где продолжил углубленное изучение этих предметов, и в 1982 окончил физико-математическую школу-интернат № 18 имени А. Н. Колмогорова при МГУ.

В 1987 окончил математический факультет Высшей школы КГБ (в настоящее время факультет известен как Институт криптографии, связи и информатики Академии ФСБ России) в Москве, где изучал математику, криптографию и компьютерные технологии, и получил специальность «инженер-математик».

В 1987 Евгений Касперский поступил на работу в многопрофильный научно-исследовательский институт при Министерстве обороны СССР. Именно здесь он начал изучать компьютерные вирусы – после того, как в 1989 столкнулся с вирусом Cascade. Проанализировав код вируса, Евгений разработал специальную утилиту для его лечения и заинтересовался данной тематикой.

В 1991 Евгений Касперский начал работать в Центре информационных технологий КАМИ, где возглавил небольшую группу специалистов, занимавшуюся разработкой антивирусных решений. В ноябре 1992 группа выпустила свой первый полноценный продукт – AVP 1.0. В 1994 он одержал победу в сравнительном тестировании, проведенном тестовой лабораторией Гамбургского университета. Это обеспечило продукту международную известность, и разработчики начали лицензировать свои технологии зарубежным IT-компаниям.

В 1997 Касперский и его коллеги приняли решение создать собственную компанию, выступив в качестве соучредителей «Лаборатории Касперского». Евгений не хотел, чтобы в названии компании фигурировала его фамилия, но его переубедила Наталья Касперская – жена Евгения на тот момент, также вошедшая в число соучредителей Лаборатории. В ноябре 2000 продукт AVP был переименован в Антивирус Касперского.

Касперский руководил антивирусными исследованиями в компании со дня её основания по 2007, когда он занял пост генерального директора «Лаборатории Касперского».

На сегодняшний день Касперский — один из ведущих мировых специалистов в области защиты от вирусов. Он является автором большого числа статей и обзоров по проблеме компьютерной вирусологии, регулярно выступает на специализированных семинарах и конференциях в России и за рубежом. Касперский — член Организации исследователей компьютерных вирусов (CARO), которая объединяет экспертов в этой области.

04 октября 1999 (15 лет назад)

В США создан центр надзора и контроля за преступностью в Internet (FS-ISAC)

США

Источник: redday.ru

Министерство Финансов США, а также ряд крупнейших банков и инвестиционных компаний: Citigroup, Bank of America, Merrill Lynch, J.P. Morgan и др. - открыли новый центр, Financial Services Information Sharing and Analysis Center (FS-ISAC). Главной функцией нового центра стало обнаружение результатов деятельности хакеров в сети и последующее оперативное извещение банков и финансовых институтов о наличии исходящей от хакеров угрозы.

Создание такого центра стало насущной необходимостью. По данным Computer Security Institute, около 64% опрошенных компаний, были подвергнуты нападениям хакеров 1998.

07 октября 1999 (15 лет назад)

Обнаружен первый в мире компьютерный вирус, внедряющийся на самый высокий уровень безопасности Windows NT — область системных драйверов

США

Источник: ru.wikipedia.org

Эта особенность делает вирус труднодоступным для лечения в памяти многими антивирусными программами.

Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведения в негодность аппаратных комплексов компьютера.

С распространением сетей и Интернета файловые вирусы всё больше ориентируются на них как на основной канал работы (ShareFun, 1997 — макровирус MS Word, использующий MS-Mail для распространения; Win32.HLLP.DeTroie, 1998 — семейство вирусов-шпионов; Melissa, 1999 — макровирус и сетевой червь, побивший все рекорды по скорости распространения). Эру расцвета «троянских коней» открывает утилита скрытого удаленного администрирования BackOrifice (1998) и последовавшие за ней аналоги (NetBus, Phase).

Вирус Win95.CIH достиг апогея в применении необычных методов, перезаписывая FlashBIOS зараженных машин (эпидемия в июне 1998 считается самой разрушительной за предшествующие годы).

В конце 1990-х — начале 2000-х годов с усложнением ПО и системного окружения, массовым переходом на сравнительно защищенные Windows семейства NT, закреплением сетей как основного канала обмена данными, а также успехами антивирусных технологий в обнаружении вирусов, построенных по сложным алгоритмам, последние стали всё больше заменять внедрение в файлы на внедрение в операционную систему (необычный автозапуск, руткиты) и подменять полиморфизм огромным количеством видов (число известных вирусов растет экспоненциально).

13 октября 1989 (25 лет назад)

Появился компьютерный вирус Datacrime, который инициировал низкоуровневое форматирование нулевого цилиндра жесткого диска, что приводило к уничтожению таблицы размещения файлов (FAT) и безвозвратной потере данных

Нидерланды

Источник: ru.wikipedia.org

Вирус Datacrime имел крайне опасное проявление - с 13 октября по 31 декабря 1989 он инициировал низкоуровневое форматирование нулевого цилиндра жесткого диска, что приводило к уничтожению таблицы размещения файлов (FAT) и безвозвратной потере данных. Первое сообщение об обнаружении вируса поступило в марте из Нидерландов от человека по имени Фред Фогель (Fred Vogel). Несмотря на небольшое распространение, Datacrime вызвал повальную истерию в мировых средствах массовой информации. Последователь-

но воспроизведенные многими печатными изданиями сведения об этом вирусе вызвали существенное искажение его реальной опасности и механизма действия. В США он даже получил название День Колумба, причем некоторые издания предположили, что вирус был написан никем иным как норвежскими террористами, пытавшимися отомстить за то, что открывателем Америки считается Колумб, а не Рыжий Эрик.

16 октября 1989 (25 лет назад)

На компьютерах VAX/VMS в сети SPAN была зафиксирована эпидемия вируса-червя WANK Worm (W.COM)

США

Источник: virusunet.narod.ru

Червь атаковал сеть NASA SPAN, через системы VAX/VMS использующие DECnet. Червь использует две особенности DECnet/VMS для того, чтобы распространяться. Первая — это учётная запись DECnet, создаваемая по умолчанию, которая предназначена для пользователей, не имеющих собственного логина в системе, и которая даёт возможность пользоваться системой более или менее анонимно. Червь использовал эту учётную запись для того, чтобы скопировать себя в систему, а затем использовал трюк с «TASK 0», для того, чтобы запустить копию в удалённой системе.

Для распространения червь использовал протокол DECNet и менял системные сообщения на сообщение "WORMS AGAINST NUCLEAR KILLERS", сопровождаемое текстом "Your System Has Been Officially WANKed". WANK также менял системный пароль пользователя на набор случайных знаков и пересылал его на имя GEMPAK в сети SPAN.

20 октября 2010 (4 года назад)

Принята государственная программа Российской Федерации "Информационное общество (2011 - 2020 годы)

Россия, Москва

Источник: gosbook.ru

Программа утверждена Распоряжением Правительства РФ от 20.10.2010 N 1815-р.

В первой версии для реализации программы предлагались следующие 6 подпрограмм: Качество жизни граждан и условия развития бизнеса в информационном обществе; Электронное государство и эффективность государственного управления; Российский рынок информационных и телекоммуникационных технологий; Базовая инфраструктура информационного общества; Безопасность в информационном обществе; Цифровой контент и культурное наследие.

Распоряжением от 2 декабря 2011 №2161-р в государственную программу Российской Федерации «Информационное общество (2011 - 2020)»

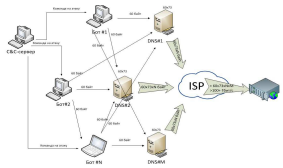
В последней версии остались 4 подпрограммы: Информационно-телекоммуникационная инфраструктура информационного общества и услуги, оказываемые на ее основе; Информационная среда; Безопасность в информационном обществе; Информационное государство.

Таким образом, за год программа отошла он заложенной в ней цели развития взаимодействия «государство-гражданин» и превратилась в очередную сухую ведомственную программу, которая, вместе с тем, активно устаревает, хотя бы уже потому, что в ней нет упоминаний о развитии сервисов «электронного голосования» и интернет-трансляций с избирательных участков, которые внедрялись на протяжении последних 4 месяцев.

21 октября 2002 (12 лет назад)

Американские спецслужбы сообщили о самой серьезной атаке на корневые DNS-серверы за всю историю Сети

США
Источник: supercook.ru



DoS-атака (атака типа «отказ в обслуживании», от англ. Denial of Service) — атака на вычислительную систему с целью довести её до отказа, то есть, создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. Отказ «вражеской» системы может быть и шагом к овладению системой (если в нештатной ситуации ПО выдаёт какую-либо критическую информацию — например, версию, часть программного кода и т. д.). Но чаще это мера экономического давления: простой службы, приносящей доход, счета от провайдера и меры по уходу от атаки ощутимо бьют «цель» по карману.

В понедельник, 21 октября 2002, Американские спецслужбы сообщили о самой серьезной атаке на корневые DNS-серверы за всю историю Сети. По информации Центра защиты национальной инфраструктуры ФБР США, во время атаки семь из тринадцати серверов, управляющих главными магистралями Интернета, перестали отвечать на запросы пользователей, работа еще двух серверов время от времени прерывалась. Атака была предпринята в понедельник 21 октября, примерно в 16:45 по времени восточного побережья США (0:45 вторника 22 октября по московскому времени). Хакеры использовали DDoS-атаку - они попытались переслать машинам значительно больше данных, чем те в состоянии обработать.

Представители компании Matrix Netsystems, которая постоянно наблюдает и отслеживает текущее состояние сети Интернет, сообщили, что машины вынуждены были обрабатывать в 30-40 раз больше информации, чем обычно. Серьезных перебоев в работе Сети не произошло лишь из-за небольшой продолжительности атаки - она длилась всего один час. Стабильности работы Интернета способствовало и то, что многие провайдеры кэшируют данные из других сегментов Сети для ускорения доступа к ним. Однако в случае более продолжительной атаки или выхода из строя большего числа корневых серверов, нормальная работа всемирной сети могла бы быть нарушена.

По информации агентства Reuters, в число наиболее сильно пострадавших от атаки root-серверов вошли компьютеры, установленные в Информационном центре министерства обороны США в городе Вена, штат Виржиния, Исследовательском центре вооруженных сил США в Абердине, штат Мэриленд, штаб-квартире ICANN в Лос-Анджелесе, Калифорния и другие. За пределами США были выведены из строя корневые серверы в Токио и Стокгольме.

24 октября 2007 (7 лет назад)

Обнаружена первая спамовая рассылка, использующая mp3-файлы

Россия, Москва
Источник: kaspersky.ru

"Лаборатория Касперского" сообщила об обнаружении первой спамовой рассылки, использующей для донесения основного рекламного сообщения до конечной аудитории аудиофайлы в формате mp3. Первые образцы подобных рассылок спам-аналитики зафиксировали в европейском почтовом трафике.

Зарегистрированный экспертами компании mp3-спам относится к категории так называемого stock-спама - спамовых сообщений, цель которых состоит в рекламе и повышении курса акций неких компаний.

Рассылка аудиозаписей в формате mp3 является следующим витком борьбы спамеров и разработчиков средств защиты от спама. Письма, зарегистрированные "Лабораторией Касперского", не содержали никакого текста, однако несли вложенный mp3-файл продолжительностью от 25 до 33 секунд. Открыв его, пользователь слышал искаженный звуковым фильтром женский голос, предлагающий купить акции некой компании под названием Exit Only Inc. Очевидно, что спамеры, завладевшие акциями этой компании, пытались таким образом поднять ее капитализацию с тем, чтобы впоследствии выгодно продать эти акции по возросшей цене.

Вероятно, что данная рассылка явилась для спамеров своего рода пробным камнем, и ее нельзя назвать удачной в силу некоторых технических ограничений. Из-за необходимости сделать спамовые письма как можно более компактными злоумышленники были вынуждены использовать аудиозапись очень низкого качества, поэтому слушателям очень трудно разобрать текст послания даже на самой высокой громкости. Кроме того, чтобы обойти антиспамовые фильтры, отправители несколько изменяют запись в каждом письме, от чего ее восприятие ухудшается еще больше.

26 октября 2001 (13 лет назад)

Впервые был обнаружен вирус Червь Klez - почтовый червь, проникающий на компьютер по сети или через электронную почту, используя в защите IFrame браузера Internet Explorer брешь

США
Источник: ru.wikipedia.org

Klez (сетевой червь) - почтовый червь, проникающий на компьютер по сети или через электронную почту, используя в защите IFrame браузера Internet Explorer брешь,которая допускала автоматический запуск вложенного файла (компания Microsoft исправила эту ошибку в программе Internet Explorer версий 5.01 и 5.5).

Для вируса характерна встроенная функция поиска и подавления антивирусного программного обеспечения. Принцип действия червя Klez таков: попадая в компьютер он начинает сканирование жестких дисков, затем дописывает свой код к одному из документов на зараженной машине и начинает массовую рассылку по всем найденным адресам. Вдобавок ко всему к вложению присоединялся список всех обнаруженных на зараженном компьютере адресов электронной почты. Кроме рассылки своих копий, червь обнаруживал себя по 13-м числам четных месяцев или шестым нечетных, в зависимости от модификации: в такой день все файлы на зараженных компьютерах заполнялись случайным содержимым.

Интернет-червь "Klez" является несомненным лидером по количеству вызванных инцидентов в 2002. С момента обнаружения он не выходил из списка наиболее распространенных угроз. В истории компьютерной вирусологии еще ни разу не случалось, чтобы вредоносная программа смогла так долго продержаться на высших позициях "десятки". Однако в течение года свирепствовали лишь две из десяти существующих разновидностей этого червя - "Klez.H" (обнаружен 17.04.2002) и "Klez.E" (обнаружен 11.01.2002). В общей сложности каждые 6 из 10 зарегистрированных случаев заражения были вызваны "Klez".

27 октября 1995 (19 лет назад)

Гостехкомиссией при Президенте РФ утвердила Положение о сертификации средств защиты информации по требованиям безопасности информации

Россия, Москва
Источник: fstec.ru

Эмблема ФСТЭК России

Положение было утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 № 199.

Положение устанавливало организационную структуру Системы сертификации средств защиты информации по требованиям безопасности информации, функции субъектов сертификации, порядок сертификации, государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации, общие требования к нормативным и методическим документам по сертификации средств защиты информации.

В приложениях к настоящему Положению приведены перечень средств защиты информации, подлежащих сертификации в системе сертификации, формы заявок на проведение сертификации и продление срока действия сертификата, решения по заявке на проведение сертификации (продлению срока действия сертификата), сертификата и лицензии на применение знака соответствия.

27 октября 2003 (11 лет назад)

Запущен червь Sober (en:Sober worm), который поддерживает своё присутствие в сети до 2005 в различных вариантах

США

Источник: ru.wikipedia.org

Вредоносная программа распространялась при помощи предшествующей версии червя, "Sober.p", содержащей функцию загрузки файлов с нескольких интернет-сайтов. Таким образом, новый червь поражал лишь те компьютеры, которые уже заражены "Sober.p". "Sober.q" представляет собой модификацию исходного кода почтового червя Email-Worm.Win32.Sober, однако не содержит функции распространения своего тела в виде вложенных в письма файлов.

Вместо этого, программа рассылает по электронной почте различные тексты и ссылки радикально-политического характера.Будучи запущенным и активизированным на атакуемом компьютере своим предшественником, "Sober.q" копирует себя в системный каталог Windows и регистрирует себя в ключе автозапуска системного реестра и ключе, отвечающем за запуск исполняемых файлов. Таким образом, червь получает управление при каждом запуске любого исполняемого файла в зараженной системе. Помимо этого, он создает несколько вспомогательных файлов с разными именами в системном каталоге Windows. Затем "Sober.q" сканирует файловую систему пораженного компьютера и записывает в специальные файлы все найденные адреса электронной почты, за исключением принадлежащих крупным разработчикам антивирусного и прочих видов программного обеспечения. Далее вредоносная программа производит ряд действий, не вписывающихся в стандартный алгоритм действий червей семейства Sober.

Вирус создает файл под названием %system%\Spammer.ReadMe и следующим текстом на немецком языке. Затем вредоносная программа рассылает по всем найденным адресам, относящимся к доменным зонам de, ch, at, li и gmx письма с текстами радикально-политического толка на немецком языке, отправляя по всем прочим адресам англоязычные послания. В теле червя содержится несколько десятков различных вариантов текстов для рассылок такого рода. Наконец, аналогично предыдущим вариантам червя, "Sober.q" путем обращения к нескольким NTP-серверам регулярно проверяет системное время. В случае, если дата соответствует 11 мая 2005 года либо является более поздней, вредоносная программа пытается загрузить произвольные файлы с нескольких интернет-ресурсов. Также, "Sober.q" пытается обнаружить в памяти и прекратить работу приложений, содержащих в названии следующие строки:microsoftanti, gcas, gcip, giantanti, inetupd, nod32kui, nod32, fxsob, s-t-i-n-g, hijack, sober.

30 октября 2007 (7 лет назад)

Мэром Москвы утвержден пакет документов по вопросам защиты информации в информационных системах города

Россия, Москва

Источник: garant.ru

Герб Москвы

Информационные системы органов исполнительной власти города Москвы рассматриваются в документах как автоматизированные системы (АС). Утвержденные документы носят обязательный характер для всех органов власти и государственных организаций города Москвы.

Мэром Москвы были утверждены:

1) Положение о порядке проведения контроля защищенности информационных систем и ресурсов города Москвы

Положение устанавливает организацию и порядок проведения контроля защищенности информационных систем (ИС) города Москвы, находящихся в эксплуатации.

2) Положение о порядке организации и проведения работ по защите конфиденциальной информации при ее автоматизированной обработке

Защита конфиденциальной информации в информационных системах и ресурсах (ИСиР) органов исполнительной власти и организаций города Москвы является составной частью мероприятий, проводимых в рамках информатизации органов государственного управления города Москвы, муниципальных образований города, организаций и предприятий города Москвы, и осуществляется в соответствии с законодательством и требованиями нормативно-технических документов в области защиты информации. Положение устанавливает порядок работ по защите конфиденциальной информации при ее автоматизированной обработке на этапе эксплуатации ИСиР.

3) Положение о порядке разработки систем защиты информации в информационных системах города Москвы

Положение устанавливает организацию и порядок разработки систем защиты информации в информационных системах (ИС) города Москвы. Система защиты информации (далее – СЗИ) представляет собой комплекс организационных мер и программно-аппаратных средств обеспечения безопасности информации (защиты информации), включаемых в ИС. Действие настоящего Положения распространяется также на работы, связанные с модернизацией ИС и СЗИ.

4) Положение о порядке эксплуатации систем защиты информации в информационных системах города Москвы

Положение устанавливает организацию и порядок эксплуатации систем защиты информации в информационных системах города Москвы. Положением выделен следующий комплекс эксплуатационных мероприятий: осуществление руководства работами по обеспечению защиты информации; обеспечение кадровой политики организации в отношении СЗИ; выполнение работ по физической защите технических средств; техническое обслуживание и ремонт оборудования; сопровождение программного обеспечения; устранение неисправностей программных и технических средств; контроль выполнения установленных нормативными документами требований к эксплуатации СЗИ.

5) Положение по аттестации информационных систем города Москвы по требованиям безопасности информации

Положение устанавливает основные принципы, организационную структуру системы аттестации, порядок проведения аттестации, а также контроля и надзора за аттестацией объектов информатизации информационных систем органов исполнительной власти города Москвы.

31 октября 1999 (15 лет назад)

Октябрь 1999 принес компьютерному сообществу три неприятных сюрприза - вирус "Infis", многоплатформенный вирус для MS Project и скрипт-вирус "Freelinks"

США
Источник: smallsecret.narod.ru

Во-первых, был обнаружен вирус "Infis", который стал первым вирусом для этой операционной системы, внедряющийся на самый высокий уровень безопасности платформы - область системных драйверов. Эта особенность делает вирус труднодоступным для лечения в памяти антивирусными программами.

Во-вторых, в конце месяца антивирусные компании сообщили о первом компьютерном вирусе для MS Project. В действительности, это был многоплатформенный вирус, одинаково успешно заражавший как файлы MS Word, так и MS Project.

В-третьих, проявился известный еще с июля скрипт-вирус "Freelinks", привлекший внимание вирусописателей к языку программирования Visual Basic Script (VBS) и ставший одним из предшественников печально известного вируса LoveLetter.

31 октября 2012 (2 года назад)

Представленная новая версия DLP-системы Zecurion Zlock шифрует файлы при записи на USB-устройства

Россия, Москва
Источник: zecurion.ru

Zecurion Zlock 5.0 впервые среди DLP-систем включает в себя функционал по защите конфиденциальных файлов на USB-устройствах с помощью шифрования — криптопериметр.

Криптопериметр — уникальная функция для DLP-систем — является принципиальным отличием Zlock от существующих на рынке решений для защиты конечных точек сети от утечек. Криптопериметр позволяет нейтрализовать широкий спектр угроз: сотрудники могут беспрепятственно копировать конфиденциальные документы на флешки и работать с ними на авторизованных компьютерах, а при утере, краже или использовании носителя третьими лицами зашифрованные файлы будут надежно защищены от несанкционированного доступа.

СПРАВОЧНЫЕ РАЗДЕЛЫ

Справочник по регионам

Справочник по источникам информации

НОВЫЕ ИЗДАНИЯ 2015 ГОДА:

- АВТОМАТИЗАЦИЯ. РОБОТОТЕХНИКА
- АХО: УПРАВЛЕНИЕ, ТЕХНОЛОГИИ, ПРАКТИКА
- ВЕСТНИК БИОТЕХНОЛОГИЙ
- ИТ-СТРАТЕГИЯ В БИЗНЕСЕ
- ПСИХОЛОГИЯ БИЗНЕСА: ПРАКТИЧЕСКИЕ РЕШЕНИЯ
- СОВРЕМЕННЫЙ ГОРОД: ПРАКТИЧЕСКИЕ РЕШЕНИЯ
- ЭЛЕКТРОНИКА. ЭЛЕКТРОТЕХНИКА

...Как правило, наибольшего успеха добивается тот,
кто располагает лучшей информацией...

Бенджамин Дизраэли (1804-1881)
— английский государственный деятель Консервативной партии Великобритании,
40-й и 42-й премьер-министр Великобритании

НОВИНКИ * ОБЗОРЫ * АНАЛИТИКА * РЕЙТИНГИ * ТРЕНДЫ * ЭКСПЕРТИЗА

ТРЕНДЫ * ЭКСПЕРТИЗА * НОВИНКИ * ОБЗОРЫ

НОВИНКИ * ОБЗОРЫ * АНАЛИТИКА * РЕЙТИНГИ

ТРЕНДЫ * ЭКСПЕРТИЗА * НОВИНКИ * ОБЗОРЫ * АНАЛИТИКА * РЕЙТИНГИ

Периодичность выхода Ежемесячно
Учредитель ООО «Гротек»
Генеральный директор Андрей Мирошкин
Издатель Информационное агентство «Монитор»
Руководитель агентства Татьяна Никонова
Свидетельство о регистрации СМИ ИА № 77-1095
Тираж Менее 1000 экз.

Подписка по каталогам в отделениях Почты России:
Газеты и журналы индекс **46664**
Пресса России индекс **41746**
Почта России индекс **63458**

Почта: 123007, Москва, а/я 82
Телефон: (495) 647-0442 Факс: (495) 221-0862
Подписка: monitor@groteck.ru www.icenter.ru
Редакционное сотрудничество: monitor@groteck.ru

iCENTER.ru