На рынке СМИ
с 1992 года

Groteck
Business Media

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

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 (70) 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:

Зарубежная практика

Соглашения и партнерства. Сотрудничество. Обмен опытом

АНОНСЫ

Новинки профессиональной литературы

Обучение / повышение квалификации

Деловой календарь

ИСТОРИЧЕСКИЙ РАКУРС: ОКТЯБРЬ

СПРАВОЧНЫЕ РАЗДЕЛЫ

ЦИТАТЫ НОМЕРА

АЛЕКСАНДР ЖАРОВ
Руководитель, Роскомнадзор

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.

АЛЕКСЕЙ ОСЬКИН
Руководитель отдела технического и маркетингового сопровождения, ESET Russia

Чем меньше информации о себе вы оставляете в сети, тем меньше шансов на то, что нежелательные сведения попадут в открытый доступ. Если вы активно общаетесь онлайн, регулярно проверяйте настройки конфиденциальности аккаунтов в соцсетях, освобождайте почтовые ящики от старых писем и используйте сложные неповторяющиеся пароли для всех веб-сервисов.

ГРЭМ КЛУЛИ
Эксперт по информационной безопасности, Eset

Давным-давно, когда о DLP 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.

ВЛАДИМИР УЛЬЯНОВ
Руководитель аналитического центра, Zecurion

Компании чаще всего узнают об утечках информации, только когда эта информация где-то всплывает или становятся заметными негативные последствия инцидента. Виной тому низкий уровень проникновения серьёзных корпоративных средств ИБ, в частности, DLP-систем. Даже в крупных компаниях вопросам информационной безопасности зачастую не уделяется должного внимания.

ЦИФРЫ. ПРОГНОЗЫ НОМЕРА

тысяч аккаунтов заблокировал в качестве превентивной меры «ВКонтакте» из-за утечки более 10 млн учетных записей и паролей электронных почтовых ящиков.

млн изображений лиц людей будет содержать к концу 2015 г. инновационная система слежения за гражданами в США, включая простых прохожих, не замешанных в каких-либо преступлениях.

млн клиентов Интернет-сервиса бронирования туристических туров Viator, используемого приложением TripAdvisor, оказались скомпрометированы из-за утечки персональных данных.

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.

млн евро в рамках проекта «Укрепление информационного общества в Украине» предоставят Совет Европы и Евросоюз. Полученные средства будут направлены на техническую и экспертную помощь.

тысячи образовательных организаций публиковали персональные данные учеников на своих официальных сайтах. Роскомнадзор обнаружил нарушения и потребовал их устранить.

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.

РОССИЙСКОЕ РЕГУЛИРОВАНИЕ

Законодательные акты и инициативы

Интернет-отрасль подготовит разъяснения по хранению персональных данных в России

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

Сергей Гребенников, замруководителя РАЭК

Российская ассоциация электронных коммуникаций /РАЭК/, объединяющая крупнейших игроков интернет-рынка России, создаст рабочую группу для разработки концепции по развитию отрасли хранения и обработки информации в российских дата-центрах в связи с принятием закона о хранении персональных данных россиян на территории РФ, говорится в сообщении РАЭК. Одним из направлений работы группы станет разработка рекомендаций и разъяснений по спорным положениям ФЗ 242 "О внесении изменений в законодательство о защите персональных данных". Основной задачей группы станет формирование предложений по стимулированию отрасли, чтобы зарубежным интернет-компаниям было удобно здесь работать, пояснил ИТАР-ТАСС замруководителя РАЭК Сергей Гребенников.

По его словам, зарубежные компании выбирают другие страны для своих серверов из-за отсутствия в России законодательных гарантий защиты данных интернет-пользователей, с которыми они работают. Результаты будут направлены депутатам Госдумы, Минкомсвязи, Роскомнадзору через две недели. "Закон создает дополнительную нагрузку на бизнес, на регуляторов, влечет дополнительные расходы и таким образом может негативно повлиять на ВВП", - считают в РАЭК. В июле 2014 года президент России Владимир Путин подписал закон, обязывающий интернет-компании размещать персональные данные о российских пользователях на серверах на территории РФ. Новые требования вступят в силу с 1 сентября 2016 года. Как указано в законе, "при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение /обновление, изменение/ извлечение персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ". В законе предусмотрены санкции за нарушения. Так, доменные имена и сетевые адреса, которые не будут соблюдать положения закона, предлагается вносить в специальный "Реестр нарушителей прав субъектов персональных данных". Вести его должен Роскомнадзор, а основанием для включения в список, как предполагается, будет имеющий законную силу судебный акт. Нарушение закона также повлечет ограничение доступа к данному информационному ресурсу. После устранения нарушений доступ будет вновь восстановлен.

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.

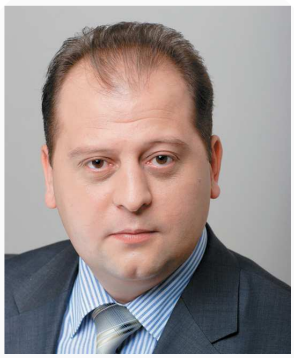
Практика правоприменения продемонстрировала, что обработка персональных данных в государственных и муниципальных информационных системах не всегда требует обезличивания информации. Необходимость применения указанной меры защиты возникает в исключительных случаях, которые установлены российским законодательством. 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

Андрей Прозоров, ведущий эксперт InfoWatch по информационной безопасности

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

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 России может появиться совет для защиты Рунета от вмешательства государства

02 октября 2014, Россия, Москва
Источник: the-village.ru

Дмитрий Мариничев, уполномоченный по делам интернета

В России может появиться экспертный совет для защиты Рунета от излишнего госрегулирования. Об этом уполномоченный по делам интернета Дмитрий Мариничев рассказал TJournal.

Предполагается, что отраслевой совет IT-рынка будет фильтровать продвигаемые властями нововведения и передавать чиновникам встречные предложения по лучшей реализации тех или иных инициатив. При этом в отличие от Российской ассоциации электронных коммуникаций и Ассоциации предприятий компьютерных и информационных технологий эта организация не будет лоббироваться какими-то определёнными компаниями, обещает Мариничев. Вместо этого, по словам омбудсмена, ей предстоит отстаивать права всей отрасли.

В качестве одного из примеров, когда участникам IT-рынка необходимо наличие третьей объективной стороны, Мариничев привёл ситуацию с переносом сроков вступления в силу закона об обязательном хранении персональных данных россиян на территории страны. Изначально документ должен был вступить в силу 1 сентября 2016 года, однако затем дату начала его действия сдвинули на 1 января 2015 года. Это оказалось на руку центрам обработки данных, но создало дополнительные трудности для большинства интернет-компаний. При этом и те и другие являются участниками одной отрасли.

Мариничев планирует передать предложение о создании нового экспертного совета президенту России Владимиру Путину. Это произойдёт 7 октября на очередной встрече представителей крупнейших российских интернет-компаний, среди которых будут «Яндекс», Mail.Ru Group и Rambler & Co.

С 1 января 2015 года операторам персональных данных будет запрещено хранить данные граждан России за рубежом

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

С 1 января 2015 года операторам персональных данных будет запрещено хранить данные граждан России за рубежом. Такая перспектива тревожит не только IT-компании, но и наиболее продвинутые отечественные банки, успевшие освоить облачные технологии. Портал Банки.ру выяснял, как новый закон отразится на банковской отрасли и во что выльется банкам уход из облаков.

24 сентября Госдума приняла во втором чтении законопроект, в соответствии с которым срок запрета на хранение персональных данных россиян за рубежом переносится на 1 января 2015 года. Изначально предполагалось ввести этот запрет в сентябре 2016 года. 29 сентября Ассоциация предприятий компьютерных и информационных технологий (АПКИТ) направила министру связи России Николаю Никифорову и спикеру Госдумы Сергею Нарышкину письмо с призывом остановить принятие спорного законопроекта.

По мнению ведущих российских IT-компаний, такое скорое вступление закона в силу может привести к приостановке деятельности большинства из них, что нанесет непоправимый ущерб экономике России. Их позиция выглядит обоснованно: облачные технологии, обеспечивающие в ряде случаев существенную выгоду, успели глубоко проникнуть в бизнес, но внутренний российский рынок облачных услуг развит пока недостаточно.

На заседании Совета безопасности, прошедшем 1 октября, Владимир Путин заявил, что Россия не планирует ограничивать доступ в Интернет и ставить его под контроль, а последние законодательные инициативы направлены на защиту отечественных информационных ресурсов. «Следует качественно повысить защищенность отечественных сетей связи и информационных ресурсов, в первую очередь тех, что используют госструктуры. Нужно стремиться исключить незаконное вмешательство в их работу, а также утечку персональной и конфиденциальной информации», – сказал президент РФ. Это позволяет предположить, что законопроект о защите персональных данных находится полностью в русле государственной политики и никакие воззвания коммерческих структур против его принятия эффекта не возымеют.

Суть облачных технологий можно объяснить в нескольких словах – это данные и вычислительные ресурсы, доступные удаленно, через Интернет. Компания – провайдер услуги выделяет клиентам определенную долю ресурсов, которую можно при необходимости варьировать. Все заботы по построению, обслуживанию, ремонту, модернизации инфраструктуры (а в ряде случаев также по установке, обновлению и обслуживанию программного обеспечения) ложатся на плечи провайдера. Нет необходимости закупать дорогостоящее оборудование, нанимать на работу массу высококвалифицированных IT-

специалистов, вкладываться в периодическую модернизацию оборудования и программного обеспечения – нужно просто вносить абонентскую плату.

Банки «облачная мода» также не миновала, но мощным тормозом для них стали требования безопасности. Вполне очевидно, что провайдер облака при желании может получить доступ к любым данным любого клиента, а для банка это может быть критично. Кроме того, банки далеко не всегда готовы полагаться на сторонние компании в аспекте непрерывности бизнеса – не всякий облачный провайдер может гарантировать необходимую банку бесперебойность работы систем. Тем не менее, если в кредитной организации имеются развитые информационные системы, выгода ухода в облака очевидна, а банки деньги считать умеют. Правда, не каждая финансовая организация признается в том, что отдает данные клиентов на сторону.

Радикальным решением вопроса стали частные облака, когда облачный провайдер создается самим банком и находится под полным его контролем. Но это имеет смысл для очень крупных банков или банковских групп. Банкам поменьше, желающим не отставать от прогресса в информационных технологиях, все-таки приходится сдаваться на милость сторонних компаний. При этом для защиты данных (в том числе и от самого провайдера) применяются различные криптографические решения. Об одном из таких решений мы писали.

Главный руководитель службы IT-архитектуры прикладных систем Лето Банка (группа ВТБ) Сергей Чиков рассказал порталу Банки.ру, как использует облака эта кредитная организация: «Лето Банк использует облачные решения для обеспечения внутренней IT-инфраструктуры и карточного процессинга. К первой категории относятся корпоративная почта Office 365, SharePoint Online – как ресурс для части внутреннего документооборота и корпоративного портала, Lync Online – в качестве корпоративного коммуникатора, InTune – для обеспечения управляемости и поддержки удаленных точек присутствия банка. Помимо этого, облачная инфраструктура используется для лицензирования функционала рабочих станций сотрудников – офисный пакет MS Office мы также получаем и активируем из облака Office 365. В «облачном» формате в банке реализована часть сервиса телефонии. Центр обработки данных банк также использует полностью по аутсорсинговой схеме. Большая часть облачных сервисов предоставляется компанией Microsoft (Office 365). Аутсорсинг инфраструктуры выполняет компания «Инфосистемы Джет». Услуги карточного процессинга оказывает компания «Мультикарта». Существующие бизнес-процессы в банке не предусматривают хранение персональных данных клиентов за пределами РФ».

Проще всего для банка стать клиентом крупного облачного провайдера, который обеспечит требуемую надежность работы и защищенность информации. Но сооснователь компании Parallels, старший вице-президент по разработке линейки Parallels Automation (популярной платформы для облачных сервисов) Олег Мельников считает, что эта практика в банковском секторе массовой быть не может: «Я бы сказал, что те банки, которые стали пользоваться сервисами публичных облаков (SalesForce / SugarCRM, Dropbox и прочими), – это большие бунтари. Они заметно выбиваются из ряда финансовых организаций своими передовыми, но в то же время рискованными действиями. В этой индустрии принято создавать собственные облака, свои дата-центры со своими, может быть, облачными приложениями, но исключительно для использования внутри сотрудниками. Прибегать к использованию публичных облачных сервисов – это не удел банковского сектора».

<<...Получается, что настороженное отношение банков к облакам полностью оправданно, а связанные с ними риски растут с каждым днем...>>

Тем не менее «бунтари» у нас нашлись. Об этом нам рассказывал председатель совета директоров Юниаструм Банка Георгий Писков. Его банк использует CRM-систему (систему управления взаимоотношениями с клиентами) американского облачного провайдера SalesForce, причем в этом случае применяется модель SaaS – Software as a service, программное обеспечение как услуга. То есть банк получает доступ не к облачной инфраструктуре, а к установленной в облаке программе. Очевидно, что никакие технологии защиты данных от доступа самого провайдера тут неприменимы.

По мнению Юниаструм Банка, риск того, что SalesForce выдаст данные клиентов банка каким-либо госслужбам США, полностью оправдывается экономической выгодой. В интервью порталу Банки.ру Георгий Писков сказал: «Я не уверен, что от этого надо защищаться. Коллективная безопасность, участие в ней – это обязанность каждого, не надо этого бояться. Другое дело, что органы могут быть коррумпированные или некоррумпированные, но в таком случае, как говорится, против лома нет приема. Поэтому я против того, чтобы защищаться от доступа полиции или ФСБ, или каких-то органов безопасности. Мы должны с ними конструктивно сотрудничать».

Очевидно, наше государство полагает иначе, и законопроект, запрещающий хранение персональных данных граждан России за рубежом, направлен именно против такой практики. По мнению Мельникова, найти замену SalesForce банку будет очень непросто: «В России нет компании уровня SalesForce, которая могла бы взять на себя CRM-обслуживание из облака. Есть провайдеры облачных CRM, но меньшего масштаба и, естественно, другой функциональности. То есть для IT-службы банка, которая однажды взяла на себя смелость перенести данные к западному облачному провайдеру, встает необходимость либо создать соответствующую in-house-систему, либо проводить аудит существующих провайдеров. Это обернется не столько большими инвестициями, сколько огромной головной болью для их IT-служб. Придется обратно переносить данные, уже однажды перенесенные на сторону публичного зарубежного провайдера, для многих тысяч клиентов. Нужно будет перенести все бизнес-процессы, настроенные в SalesForce, в систему российского происхождения. Кроме того, нужно будет повторно обучить сотрудников, использующих облачную CRM-систему, новой логике программного обеспечения и процессам».

Георгий Писков не считает большой проблемой перспективу вынужденного переноса систем из облаков. «Запрет на хранение персональных данных за рубежом – вообще говоря, явление не новое, аналогичные законы действуют и во Франции, и в Германии. Так что принятие такого закона в России вполне логично. Поскольку использование банками зарубежных облачных сервисов не носит тотального характера, общее воздействие этого закона на российскую банковскую систему будет незначительным и коснется небольшого количества игроков, – поясняет Писков. – Некоторые банки пойдут по пути переноса данных в российское облако, кто-то выберет шифрование данных, а кто-то часть данных, тех, что подпадают под понятие персональных, будет хранить в России, а остальное – в зарубежном облаке. Это, конечно, добавляет банкам работы, но не является фатальным явлением ни в коей мере. Банки привыкли к оперативной доработке своих систем в условиях динамично меняющегося законодательства».

В спорах об облаках следует учитывать также опасность секторальных санкций со стороны США. Одно дело, когда американским поставщикам оборудования и программного обеспечения запрещают работать с российскими банками – по большей части это лишь приведет к затруднениям при обновлении «железа» и программного обеспечения. Другое дело, когда сотрудничество разрывает облачный провайдер. Тут банку придется спешно строить собственную инфраструктуру либо искать замену провайдеру, предпочтительнее всего отечественную.

<<...Радикальным решением вопроса стали частные облака, когда облачный провайдер создается самим банком и находится под полным его контролем. Но это имеет смысл для очень крупных банков или банковских групп...>>

«Насколько широко будут распространены американские санкции, можно гадать только на кофейной гуще, но если дойдет до отключения Интернета и облачных сервисов, то очевидно, что нам придется жить в рамках уже совсем другой парадигмы. Отмечу, однако, что емкость российских ЦОДов (центров обработки данных. – Прим. ред.) сейчас вполне достаточна, чтобы обслужить немедленные нужды банковской системы», – говорит Георгий Писков.

Получается, что настороженное отношение банков к облакам полностью оправданно, а связанные с ними риски растут с каждым днем. И речь идет не только о нашей стране. «Если говорить о тенденциях, то стремление к большему контролю данных характерно далеко не только для России, – рассказал порталу Банки.ру Олег Мельников. – За последние два года, особенно после истории Сноудена, я вижу движение обратно, когда компании из разных областей экономики сначала переехали на Microsoft Azure или на Amazon S3, разработчики устремились в DigitalOcean (популярные облачные системы. – Прим. ред.), а потом потихонечку оттуда съехали на своего локального провайдера. У нас есть несколько европейских клиентов-телекомов, которые потихоньку начали переводить своих клиентов обратно в свой датацентр, потому что поняли: если сегодня в стране у них такого закона нет, то, скорее всего, в ближайшее время он появится».

Сертификация. Лицензирование. Стандарты

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.

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.>>

«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».

ЗАРУБЕЖНОЕ РЕГУЛИРОВАНИЕ

Герб Украины

Ликвидирована Госслужба Украины по вопросам защиты персональных данных

24 сентября 2014, Украина
Источник: chp.com.ua

16 сентября вступило в силу постановление Кабинета Министров Украины № 442 об оптимизации системы центральных органов исполнительной власти. Документом, в частности, ликвидирована и Государственная служба по вопросам защиты персональных данных. Функции ликвидированных органов власти возложены на профильные министерства и другие службы. Напомним, что Госслужба по защите персональных данных некоторое время выполняла функции надзора за соблюдением законодательства в сфере защиты персональных данных, в частности, проводила регистрацию баз персональных данных. В июле 2013 года часть ее функций были переданы Уполномоченному Верховной Рады по правам человека

Ради национальной безопасности Китай запретит использовать своим чиновникам смартфоны от таких производителей, как Apple и Samsung

25 сентября 2014, Китай
Источник: south-insight.com

Крупные китайские конкуренты Huawei Technologies Co Ltd и ZTE Corp, а так же Lenovo Group Ltd уже заявили о том, что возьмут долю рынка Apple и Samsung на себя.

Huawei Technologies Co Ltd, основаная в Шэньчжэне, ориентируется на защиту данных и на анти-подслушку, в своих девайсах.

Lenovo, крупнейший в мире производитель персональных компьютеров и набирающий обороты в мобильном секторе,использует в своих смартфонах систему зашиты в виде распознавания речи владельца и сканирования отпечатков пальцев. Тем самым запрет даст новый стимул китайским производителям мобильных телефонов.

Толчком к развитию таких событий послужило расследование дела об Эдварде Сноудане и слежки правительства США.

В Шанхайском муниципалитете уже заявили, что все чиновники перешли на использование китайского флагмана Huawei.

Европейские эксперты предлагают Грузии механизм «двух ключей» для прослушивания

26 сентября 2014, Грузия
Источник: apsny.ge

Герб Грузии

Эксперты Совета Европы предлагают Грузии новую модель, т.н. систему "двух ключей" в связи с механизмами доступности секретных оперативно-следственных прослушиваний.

Джозеф Канатач и Грэхем Саттон советуют группе, работающей над данной темой, если ключ тайного прослушивания будет у МВД, второй ключ передать частному провайдеру или специальной службе мониторинга. По их мнению, такой механизм в большей мере обеспечит защиту от незаконных прослушиваний.

По сообщению агентства "Интерпрессньюс", Джозеф Канатач и Грэхем Саттон ознакомили СМИ со своим видением на пресс-конференции, проведенной после двухдневных встреч в парламенте.

"Система одного ключа неприемлема. Наш совет, чтобы ключей было больше одного. Второй ключ должен быть в других руках, а не в руках Министерства внутренних дел. Второй ключ должен быть использован для перепроверки тогда, когда будет выдано разрешение суда о включении в коммуникации, и Министерство внутренних дел использует свой ключ. Второе ведомство, где будет решено хранить второй ключ, должно иметь возможность, перепроверить действительность постановления, на самом ли

деле оно было выдано судом. Местом, где будет храниться второй ключ, может быть частный провайдер, специальное агентство мониторинга"- заявил Джозеф Канатач.

По их же предложению, ни один ключ не будет действовать независимо, оба ключа должны быть задействованы во время входа в систему и подключения к прослушиванию.

Кроме того, по сообщению экспертов Совета Европы, еще одним предметом дебатов являлись т.н. "черные ящики" и необходимость их существования. По их словам, "могут существовать "черный ящик" и ключи, и может быть система ключа без "Черного ящика".

"Система, о которой говорит Министерство внутренних дел, не исключает возможности незаконного подключения к коммуникации. Вообще, никакая система не может исключить этого, и ни одна система не дает стопроцентные механизмы защиты. Предложение МВД улучшает существующее ныне положение, но это неполный шаг"- заявил Джозеф Канатач на пресс-конференции.

Предложение Министерства внутренних дел состоит в усилении надзирательской роли инспекторов охраны персональных данных. По заявлению заместителя министра внутренних дел Левана Изория, всю информацию следует передать инспектору, и дать ему возможность надзора и контроля процесса.

Евросоюз профинансирует медиареформы в Украине

02 октября 2014, Евросоюз
Источник: telegraf.com.ua

Совет Европы и Евросоюз предоставят 2,75 млн евро в рамках проекта "Укрепление информационного общества в Украине".

Полученные средства будут направлены на техническую и экспертную помощь в трех направлениях: медиа, защита персональных данных и интернет-управление.

Кроме того, в Европейском Союзе намерены выделить средства на развитие общественное вещание. ЕС так же профинансирует образовательные мероприятия о правах человека онлайн.

Реформы в медиа-сфере являются одним из обязательств, которые Украины должна выполнить в рамках Соглашения об ассоциации перед Советом Европы.

Данный проект будет реализован до января 2015 года. В это же время запланирован запуск общественного телевидения.

ПРОБЛЕМЫ. КОНФЛИКТЫ. ИНЦИДЕНТЫ

Проверки регуляторов

Арбитражная практика: Передача персональных данных третьему лицу с целью взыскания просроченной задолженности признана незаконной

08 сентября 2014, Россия, Кемеровская обл.
Источник: ibusiness.ru

Законодательством запрещена (за рядом исключений, особо оговоренных в законах) передача персональных данных третьим лицам без согласия субъектов персональных данных (то есть нас с Вами). Соответственно граждане, сталкиваясь с такими фактами, все чаще обращаются за защитой своих прав в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

В августе 2013 года Арбитражный суд Кемеровской области рассмотрел дело № А27 – 5075?2013 в котором, установив, что ОАО «МТС» по агентскому договору передало ООО «Долговое агентство «Пристав»» конфиденциальную информацию о клиенте для взыскания с гражданки просроченной задолженности по договору, признал такую практику незаконной.

Девять из десяти автодилеров Тюменской области нарушили закон о персональных данных

02 октября 2014, Россия, Тюменская обл.
Источник: t-l.ru

Десять интернет-ресурсов автодилерских организаций Тюмени проверили специалисты управления Роскомнадзора по Тюменской области, Ханты-Мансийскому автономному округу – Югре и Ямало-Ненецкому автономному округу.

В девяти из них установлены признаки нарушения законодательства в области персональных данных, из них восемь тюменских - ООО "Альянс Мотор Тюмень", ООО "ТЕХНОКОМ-ИНВЕСТ", ООО "ЕвроАзия-Сервис", ООО "Автоград Гарант", ООО "Автоград Сол", ООО "Торговый дом Автоград", ООО "Автоград Престиж", ООО "УГА-Авто" и одно ООО "Юнимоторс" Нового Уренгоя.

Предприятия не опубликовали документы, определяющие политику в отношении обработки персональных данных, сведения о реализуемых требованиях к защите персональных данных.

По результатам проведенного мероприятия операторам направили требования об устранении нарушения, сообщает управление Роскомнадзора по Тюменской области, ХМАО и ЯНАО.

Главу городского поселения Хабаровского края наказали за публикацию личных данных жителя

02 октября 2014, Россия, Хабаровский край
Источник: mngz.ru

По постановлению Амурского городского прокурора привлечен к административной ответственности глава городского поселения за опубликование персональных данных заявителя без согласия владельца.

Амурская городская прокуратура рассмотрела обращение местного жителя, который жаловался на нарушение администрацией городского поселения "Город Амурск" требований законодательства в области персональных данных. Согласно доводам заявителя, 24.07.2014 г. на официальном сайте администрации в открытом доступе размещено его обращение, адресованное главе городского поселения, в котором указаны персональные данные жителя, сообщили РИА "АмурПРЕСС" в пресс-службе краевой прокуратуры.

В ходе проверки доводы заявителя нашли свое подтверждение. Прокуратура установила, что в разделе "Обратная связь" официального сайта администрации городского поселения "Город Амурск" размещено обращение заявителя и распространены его персональные данные: фамилия, имя, отчество, домашний адрес, номер сотового телефона.

Вместе с тем, Федеральным законом "О персональных данных" установлено, что обработка персональных данных осуществляется только с согласия их владельца. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать их третьим лицам и не распространять без согласия субъекта персональных данных.

Однако глава городского поселения "Город Амурск", приняв решение опубликовать обращение с персональными данными заявителя, нарушил требования закона, что образует состав административного правонарушения, предусмотренного ст. 13.11 КоАП РФ (нарушение установленного законом порядка сбора, хранения, использования или распространения). В связи с этим, по постановлению прокурора виновный привлечен к административной ответственности в виде штрафа.

Роскомнадзор просит удалить списки детей со школьных сайтов

03 октября 2014, Россия, Москва
Источник: nord-news.ru

Списки учащихся школ, детсадов, колледжей нельзя публиковать в открытом виде в интернете. Роскомнадзор обнаружил признаки нарушений на сайтах более 2 тыс. образовательных организаций. Ведомство начало рассылать обращения к таким организациям с требованием удалить персональные данные учеников с их официальных сайтов.

- Нарушения требований законодательства вызваны не злым умыслом, а недоразумением, в связи с неверной трактовкой определенных положений закона «О персональных данных», - заявила замглавы Роскомнадзора Антонина Приезжева. - В связи с этим было принято решение не задействовать весь

спектр имеющихся механизмов воздействия на нарушителей, а воспользоваться лишь правом уполномоченного органа требовать удаления незаконно размещенной информации.

Роскомнадзор, как уполномоченный орган в сфере защиты прав субъектов персональных данных, начал мониторинг сайтов образовательных учреждений. В России уже выявлено более 2027 подобных сайтов, где персональные данные детей и их родителей можно найти в открытом доступе.

Антонина Приезжева, замглавы Роскомнадзора

- Это, как правило, интернет-представительства школ, детских садов, интернатов, а также муниципальных образований и администраций субъектов федерации, - сообщила Приезжева на конференции «День защиты персональных данных детей».

Нередко обнаруженные данные содержали не только имена и фамилии, но и даты рождения, место проживания, сведения о социальном статусе родителей и их принадлежности к той или иной льготной категории.

- Речь идет о многодетных семьях, матерях-одиночках, безработных родителях, детях сотрудников правоохранительных органов, детях судей, ребятах, оставшихся без попечения родителей. На одном сайте образовательного учреждения даже был опубликован список детей, направляемых на психоневрологическую комиссию, - добавила Приезжева.

Дмитрий Сокоушин, руководитель территориального управления Роскомнадзора по ЦФО

- Образовательные учреждения размещают личные данные детей в виде списков на своих официальных сайтах. В большинстве случаев публикуют фамилию, имя и отчество, наименование учебного заведения и дату рождения ребенка, - рассказал руководитель территориального управления Роскомнадзора по ЦФО Дмитрий Сокоушин.

Также, по его словам, личные данные ребенка нередко «публикуются в рамках проведенных соревнований, олимпиад и конкурсов».

Например, на официальном сайте МОУ «Лицей» (город Новомосковск Тульской области) вывешен список победителей и призеров муниципального этапа Всероссийской олимпиады школьников.

Как пояснил «Известиям» официальный представитель Роскомнадзора Вадим Ампелонский, подобного рода данные можно публиковать либо в обезличенном виде, либо присваивая субъектам персональных данных идентификационные номера.

Представители «Лицея» сообщили «Известиям», что с родителей они берут подписку о возможности распространения персональных данных. При этом на сайте не публикуются паспортные данные. Список победителей они, действительно, вывешивают. Ученики гордятся тем, что информация о их победе выложена на сайте. К тому же к сайту образовательного учреждения предъявляются требования - публиковать подобного рода информацию.

В Минобрнауки не ответили на вопрос о требованиях к сайтам образовательных организаций по поводу публикации списков учеников. Согласно утвержденным в 2013 году правилам, учебные заведения, реализующие профессиональные образовательные программы, должны обнародовать в Сети результаты приема.

- Есть порядок проведения Всероссийской олимпиады школьников. Организатор олимпиады обязан публиковать ее результаты - в том числе на своем сайте. Но Роскомнадзор говорит, что нельзя публиковать эти данные, - говорит директор школы № 4 города Нелидово Тверской области Сергей Погодин. - На прошлой неделе к нам в школу поступило предписание Роскомнадзора об удалении персональных данных учеников с сайта. Мы ответили, что родители дают нам письменное согласие на обработку персональных данных своих детей. Повторного запроса от Роскомнадзора пока не было.

Публиковать на сайте обезличенные данные результатов соревнований, по мнению Погодина, бессмысленно.

- Писать: «один мальчик пробежал 100 м за такое-то время», - это же смешно, - считает директор школы.

В Роскомнадзоре считают, что обнародовать персональные данные несовершеннолетних нельзя даже с согласия их самих или их родителей.

- Минобрнауки и Роскомнадзору нужно урегулировать возникшие противоречия, - считает сопредседатель Межрегионального профсоюза учителей Андрей Демидов.

Утечки информации. Инциденты

"ВКонтакте" заморозил более 200 000 аккаунтов, зарегистрированных на "утекшую" в сеть почту

15 сентября 2014, Россия, Москва
Источник: nn.ru

Утечка более 10 млн учетных записей и паролей электронных почтовых ящиков взбудоражила пользователей Всемирной паутины. В качестве превентивной меры «ВКонтакте» заблокировал 226 000 аккаунтов, зарегистрированных на почту, оказавшуюся в общем доступе.

«Во имя безопасности пользователей ВКонтакте администрация соцсети предприняла превентивные меры по защите аккаунтов, которые были зарегистрированы на скомпрометированные адреса почтовых гигантов», - сообщило созданное «ВКонтакте» издание об IT и бизнесе «LIVE Plus».

Всего было заморожено 226 000 персональных страниц, из которых 185 000, зарегистрированных на Mail.ru, 31 000 – на Яндекс.Почта, 10 000 – Gmail.

Напомним, 1 млн паролей почтового сервиса «Яндекс» попали в общий доступ 7 сентября. Спустя сутки в сети появились 4,6 млн паролей Mail.ru, а 9 сентября – 5 млн учетных записей вместе с кодовыми комбинациями Gmail. В компаниях заявили, что лишь незначительная часть «слитых» почтовых «ящиков» являются действующими. «Проверка показала, что менее 2% пар логинов и паролей могли быть рабочими, и при попытке взлома наша автоматическая система противодействия заблокировала бы попытки входа в аккаунты», - отчиталась команда Google в официальном блоге IT-гиганта.

С жалобой на утечку информации о почтовом аккаунте в Роскомнадзор обратились пара десятков человек, сообщается на официальном сайте надзорного органа. "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", - цитирует пресс-служба руководителя Роскомнадзора Александра Жарова. Однако, по его словам, учетная запись и пароль электронной почты не являются персональными данными, поэтому у надзорной службы нет полномочий для организации проверок в отношении интернет-компаний.

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. Представьте 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.

Хакеры похитили персональные данные 1,4 млн клиентов Viator

25 сентября 2014, Россия, Москва
Источник: anti-malware.ru

Интернет-сервис бронирования туристических туров Viator, используемый приложением TripAdvisor, сообщил о возможной утечке персональных данных 1,4 млн клиентов. В руках злоумышленников, вероятно, оказались

адреса электронной почты и пароли ещё 560 тыс. клиентов. Также скомпрометированными могут оказаться платежные данные 880 тыс. пользователей, сообщили CNews в компании Zecurion.

Возможную утечку данных обнаружили, когда сервис получил информацию извне о мошеннических транзакциях. По данным Viator, уведомление о незаконных платежах поступило 2 сентября от одной из процессинговых компаний, занимающихся обработкой электронных платежей. Viator утверждает, что незамедлительно принял исчерпывающие меры по расследованию инцидента и оценке масштабов ущерба.

«По статистике Zecurion Analytics, компании чаще всего узнают об утечках информации, только когда эта информация где-то всплывает или становятся заметными негативные последствия инцидента, — отметил Владимир Ульянов, руководитель аналитического центра Zecurion. — Виной тому низкий уровень проникновения серьёзных корпоративных средств информационной безопасности, в частности, DLP-систем. Даже в крупных компаниях вопросам информационной безопасности зачастую не уделяется должного внимания. До того момента, как это скажется на бизнес-показателях».

Подобная ситуация имела место и в случаях с хищением в последнее время реквизитов платежных карт таких организаций, как Home Depot, Target, Neiman Marcus и др., указали в Zecurion.

Хакеры украли у JPMorgan данные о 83 миллионах домохозяйств и предприятий

03 октября 2014, США
Источник: minfin.com.ua

Хакеры получили персональные данные 83 млн клиентов американского банка JPMorgan Chase. Об этом сообщается в отчете финансовой организации. Согласно документу, жертвами кибератаки стали 76 млн домохозяйств и 7 млн юридических лиц. Взлом системы защиты данных произошел летом этого года. Полученная информация о клиентах упростила доступ к средствам вкладчиков. Однако, как заявляют в банке, пока не было ни одного случая кражи денег. Персональные данные все равно могут быть использованы преступниками, считает генеральный директор компании R-Vision Александр Бондаренко.

"Данная информация может использоваться в каких-то других, более сложных видах мошенничества, связанных с так называемой кражей личности, когда злоумышленники используют разного рода информацию для того, чтобы либо подделать документы, либо проводить мошеннические операции, может быть, даже напрямую не связанные с человеком, чьи данные утекли из банка. Кроме того, если среди жертв есть достаточно серьезные и влиятельные люди, то дополнительная информация о состоянии их банковских счетов может быть также продана тем, кому эта информация нужна. На этом тоже можно заработать", — пояснил Бондаренко "Коммерсантъ FM".

В настоящее время представители банка совместно с сотрудниками правоохранительных органов проводят расследование. Как сообщают СМИ, под подозрением оказались хакеры из Восточной Европы и России. Скорее всего, преступники получили доступ к клиентской базе через компьютеры сотрудников, отметил заместитель директора департамента внедрения и консалтинга компании LETA Алексей Дашков.

"Вынести такой объем данных, используя какие-то атаки, довольно сложно. Чтобы сделать это незаметно, нужно делать это долго. Гораздо эффективнее использовать социальную инженерию. Возможно, была произведена кража каких-нибудь учетных данных одного из сотрудников, потом с помощью этих данных уже произведена атака на базу данных, которая содержит информацию контрагентов банка. Скорее всего, запросы на выгрузку данных осуществлялись частями, в этом и заключается сложность отслеживания этих утечек, потому что кажется, что это работают пользователи", — отметил Дашков.

Как отмечает газета The New York Times, утечка данных JPMorgan Chase может стать крупнейшей за последнее время. До сих пор рекордной по объему похищенных данных считалась атака хакеров на американскую компанию The Home Depot. Тогда злоумышленники похитили информацию о 56 млн клиентов.

Зимой 2014 года американский ритейлер Target объявил об утечке персональных данных 40 млн своих клиентов. Хакеры имели доступ к информации в течение двух месяцев. В их распоряжении оказались номера телефонов, электронные и почтовые адреса, номера и PIN-коды кредитных и дебетовых карт. Как сообщает газета The New York Post, преступники пользовались вредоносной программой, которую ранее написал 17-летний программист из Санкт-Петербурга. В феврале этого года группа хакеров NullCrew разместила в интернете логины, пароли, адреса электронной почты и номера кредитных карт пользователей телекоммуникационной компании Bell Canada. Жертвами киберпреступников стали более 20 тыс. клиентов оператора. Этим летом хакеры атаковали системы американской компании по доставке почты и логистике UPS Store. Вредоносные программы были обнаружены более чем в 50 отделениях фирмы, которые расположены в 24-х штатах страны. Известно, что злоумышленники получили доступ почти к 100 тыс. транзакций. Данные об операциях поставили под угрозу банковские счета клиентов компании.

Как заявили в JPMorgan Chase, ежегодно на обслуживание системы безопасности банка выделяется порядка $250 млн.

ПРОЕКТЫ. КОМПЛЕКСНЫЕ РЕШЕНИЯ. ОПЫТ ВНЕДРЕНИЯ

В Волгоградской области совершенствуют электронную систему обработки обращений граждан благодаря компании БФТ

17 сентября 2014, Россия, Волгоградская обл.
Источник: b2blogger.com

В Волгоградской области реализуется проект по созданию автоматизированной системы учета и обработки обращений граждан в рамках применяемой системы электронного документооборота, разработчиком которой является Компания БФТ.

Проект подразумевает создание единой системы документооборота, которая охватит не только все органы исполнительной власти Волгоградской области, а также обеспечит взаимодействие с федеральными, региональными министерствами и ведомствами. Проект позволит автоматизировать и значительно ускорить процесс обработки обращений граждан области.

Герб Волгоградской области

СЭД «DoXLogic» в Администрации Волгоградской области применяется с 2011 года. При этом автоматизация обработки обращений граждан до недавнего времени была только локальной: электронная обработка происходила в отделе по работе с обращениями Администрации Волгоградской области, а документооборот между подразделениями осуществлялся на бумажных носителях. В связи с высокими темпами информатизации органов власти Администрацией Волгоградской области было принято решение о модернизации электронной системы документооборота в части обращений граждан, а именно:

- обеспечения возможности учета в электронном виде рассмотрения обращений граждан органами исполнительной власти Волгоградской области в установленном законодательством порядке;

- обеспечения возможности взаимодействия СЭД «DoXLogic» с защищенной системой межведомственного электронного документооборота (МЭДО), организуемой Федеральной службой охраны Российской Федерации.

В рамках первого этапа Компанией БФТ были проведены работы по детальному обследованию процесса обработки обращений граждан и адаптации системы СЭД «DoXLogic» под требования Администрации Волгоградской области и локальных нормативно-правовых актов. Второй этап работ посвящен организации электронного документооборота Администрации области с федеральными и региональными органами исполнительной власти. Для этого будет настроено взаимодействие применяемой СЭД с системой МЭДО посредством специального шлюза, который позволит получать документы из федеральных органов власти и других субъектов РФ, подключенных к МЭДО, в электронном виде, а сотрудникам Администрации не придется вносить их в систему вручную. По завершению всех этапов проекта специалистами Компании БФТ будет проведено комплексное обучение сотрудников Администрации Волгоградской области, ответственных за работу с обращениями граждан, работе с системой.

Стоит отметить, что в соответствии с Федеральным Законом № 152-ФЗ «О персональных данных», в СЭД «DoXLogic» Администрации Волгоградской области будут использованы самые строгие меры защиты персональных данных, что исключает возможность утечки информации третьим лицам.

В ближайшее время планируется автоматизировать около 100 рабочих мест сотрудников, ответственных за обработку обращений граждан, и осуществить интеграцию СЭД «DoXLogic» с порталом Администрации Волгоградской области для автоматической передачи в систему размещенных на портале обращений и дальнейшей их обработки.

Компания Yahoo! предпримет дополнительные меры для защиты персональных данных своих пользователей

17 сентября 2014, США
Источник: svit24.net

Yahoo! уделяет много внимания безопасности. Компания предпримет дополнительные меры для защиты персональных данных своих пользователей. Об этом говорится в официальном сообщении компании, подписанном ее генеральным директором Мелиссой Майер.

Как рассказала Майер, вскоре абсолютно все данные, передаваемые между дата-центрами компании будут защищены протоколом шифрования SSL. Помимо этого, пользователям, использующим почту Yahoo!, будет предоставлена возможность использовать этот протокол для защиты своих электронных писем, отправленных на почтовые серверы других компаний.

В настоящее время Yahoo! уже использует SSL для защиты электронной переписки между пользователями своего сервиса электронной почты. Такая защита была внедрена после того, как в конце октября минувшего года в СМИ появилась информация о том, что Агентство национальной безопасности США смогло установить слежку за каналами, связывающими дата-центры Yahoo! по всему миру.

Объявление компании о дополнительных мерах безопасности последовало спустя несколько дней после судебного иска, поданного против Yahoo! в Калифорнии. Компанию обвинили в перехвате переписки клиентов ее почтового сервиса с пользователями других почтовых сервисов: собранные таким образом данные впоследствии якобы использовались для рассылки персонального спама.

В Yahoo! всегда настаивали, что конфиденциальность данных пользователей очень важна для компании. Так, в отличие от некоторых других интернет-гигантов США, таких как Apple и Microsoft, которые частично признались в сотрудничестве со спецслужбами, в Yahoo! последовательно заявляли, что никогда не предоставляли правительству доступа к пользовательским данным. Компания также обратилась в суд с требованием разрешить публикацию подробной статистики запросов о предоставлении информации со стороны спецслужб.

В Челябинской области планируется развитие информационных систем в здравоохранении

24 сентября 2014, Россия, Челябинская обл.
Источник: up74.ru

Пользу от этой работы своим примером доказал областной медицинский информационно-аналитический центр. В этом году у него юбилей — уже десять лет он занимается ведением медстатистики, обеспечением защиты при передаче персональных данных жителей и многим другим.

За время работы функции сотрудников центра постоянно дополнялись новыми. Так, в этом году здесь был введен мониторинг деятельности круглосуточного стационара. По словам Елены Рыжей, замдиректора учреждения, это позволяет анализировать заболеваемость жителей региона (как общую, так и госпитальную, и первичную).

Кстати, запись к врачу дистанционным способом также была введена в прошлом году благодаря сотрудникам центра, которые разрабатывают медицинскую информационную систему области (это в свою очередь позволяет оперативно получать информацию о работе всех медучреждений).

Сейчас в центре работают больше 40 человек, которые занимаются обработкой статистических данных. В будущем планируется развитие новых информационных систем в соответствии с требованиями рынка, увеличение штата сотрудников.

Роскомнадзор не собирается блокировать Google.com, Facebook и Twitter

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

Эмблема Роскомнадзора

Роскомнадзор сейчас ведет регистрацию интернет-площадок в основном по запросам правоохранительных органов.Причем запросы на включение в реестр делаются не обязательно потому, что ресурс нарушил букву закона, подчеркнул в беседе с "РГ" пресс-секретарь ведомства Вадим Ампелонский. Российские площадки "Яндекс", "ВКонтакте", Mail.Ru и "Рамблер" уже включены в реестр.

Почти два месяца действуют поправки в законы "Об информации, информационных технологиях и о защите информации", "О связи" и в Кодекс об административных правонарушениях (КоАП). Одно из нововведений как раз касается сайтов и систем, обеспечивающих прием, передачу, доставку и обработку электронных сообщений пользователей Сети. Такие ресурсы должны зарегистрироваться в Роскомнадзоре в качестве организатора распространения информации и в течение шести месяцев хранить "на территории России информацию о всем контенте, который проходит через их площадки.

Роскомнадзор может по собственной инициативе попросить их встать на учет. Сейчас служба ведет работу с Google.com, Facebook и Twitter по регистрации их в реестре в рамках исполнения так называемого закона о блогерах.

Роскомнадзор высылал этим компаниям уведомления о необходимости зарегистрироваться в реестре. Они направили эти обращения на юридическую экспертизу. И взяли паузу для изучения.

"Мы их не торопим. Видим заинтересованность в том, чтобы исполнять российское законодательство", - отметил Ампелонский.

Речи о санкциях по отношению к этим площадкам не идет, подчеркнул он. Но если они будут уклоняться от исполнения закона, то им в первую очередь грозит штраф в 500 тысяч рублей. Блокировка доступа к такой нерадивой площадке рассматривается только как крайняя мера.

"Также мы общаемся с ними по исполнению закона о персональных данных", - рассказал собеседник. Ведь у них должны быть серверы на территории России.

Но в целом пока компании осторожничают. Например, Twitter воспринимает Россию как достаточно важный рынок, который явно не хочет потерять, однако пока не делает заявлений об открытии здесь офиса или найме официального представителя. Российские компании относятся к требованию по предоставлению информации о пользователях нормально. И до этого правоохранительные органы могли затребовать информацию о тех, кто пишет у них на площадке. Но нужно было предписание или запрос из судебной инстанции.

Со вступлением закона для интернет-площадок изменился статус, и их приравняли к операторам связи. И теперь они должны установить дополнительное оборудование - средства для обеспечения функций оперативно-разыскных мероприятий. Это компании считают излишним, отметил эксперт. Ведь на линиях связи у операторов уже стоит такое оборудование, и получится дубляж.

Что касается площадок с участием иностранного капитала, которые ведут бизнес в России, то они не отказываются от диалога с властями. Они даже пойдут на то, чтобы организовать здесь свои серверы для хранения персональных данных, прогнозирует эксперт.

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.

НАИЗ запустил проект по защите персональных данных

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

1 октября 2014 г. эксперты «Национальной ассоциации институтов закупок» (НАИЗ) приступили к реализации социально значимого проекта «Защита персональных данных человека и гражданина». В июне этого года он победил в открытом конкурсе по выделению грантов президента России некоммерческим неправительственным организациям и получил государственную поддержку, сообщили CNews в НАИЗ.

При реализации проекта используются средства государственной поддержки, выделенные в качестве гранта в соответствии с распоряжением президента РФ от 17.01.2014 г. №11-рп и на основании конкурса, проведенного Некоммерческим фондом — Институтом социально-экономических и политических исследований (ИСЭПИ).

В рамках проекта будет создан портал по защите персональных данных, размещены плагины для интернет-браузеров, разработаны и введены в эксплуатацию функциональные приложения.

Сервисы будут позволять автоматически жаловаться на нарушения в указанной сфере в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Отдельный раздел проекта будет посвящен нарушениям в сфере защиты персональных данных при осуществлении закупок для государственных и муниципальных нужд. В этой области проект имеет особую важность для поставщиков, раскрывающих свои персональные данные в конкурсных и иных заявках, а также при предоставлении информации о конечных бенефициарах, указали в НАИЗ.

"Ростелеком" удвоит количество дата-центров в РФ, чтобы уместились все данные россиян, перенесенные из-за границы

03 октября 2014, Россия, Москва
Источник: hitech.newsru.com

Сергей Калугин, Президент "Ростелекома"

Президент "Ростелекома" Сергей Калугин заявил, что оператор будет создавать новые дата-центры, куда компании смогут перенести персональные данные россиян, сообщил "Прайм". Компания ориентируется на строительство двух очень больших и семи не очень больших дата-центров, управляться они должны российским софтом, сообщил Калугин.

Представитель "Ростелекома" Андрей Поляков подтвердил это, сообщив, что размеры центров, места их расположения и бюджет программы планируется утвердить на одном из ближайших заседаний совета директоров оператора. Сейчас у оператора семь межрегиональных и несколько региональных дата-центров меньшего масштаба, говорит он.

Согласно поправкам в закон "О персональных данных", принятым Госдумой во втором чтении, персональные данные россиян должны будут храниться на территории России уже с 1 января 2015 года, а не с 1 сентября 2016 года, как планировалось ранее. В результате в начале 2015 года спрос на дата-центры в краткосрочной перспективе вырастет на 10-20%, уверен старший аналитик IDC Михаил Попов.

Дополнительные мощности "Ростелекому" нужны, чтобы обслуживать крупных западных клиентов - например, Google, пояснил сотрудник "Ростелекома". По его словам, компания встречалась с менеджментом Google и обсуждала в том числе и возможность предоставления серверов в аренду. Представитель Google в России отказался от комментариев.

На создание дата-центра с нуля "Ростелекому" может потребоваться не менее полутора лет: полгода на проектирование и согласование и год - на реализацию проекта, говорит гендиректор Radius Group Дмитрий Мариничев. По его оценке, сейчас спрос на мощности дата-центров не превышает предложе-

ния и есть много свободных площадок. Но если западные компании начнут активно переносить данные в Россию, то понадобятся в два-три раза большие мощности, чем есть сейчас, считает он. Крупные компании могут озаботиться строительством собственных дата-центров, но в первое время им все равно придется арендовать мощности, комментирует эксперт.

Напомним, идею о том, что серверы крупных национальных компаний должны быть перенесены на территорию России в целях защиты информации, высказал в апреле президент Владимир Путин.

ПРОГНОЗ МЕСЯЦА:

Михаил Попов, IDC, старший аналитик, Россия, Москва

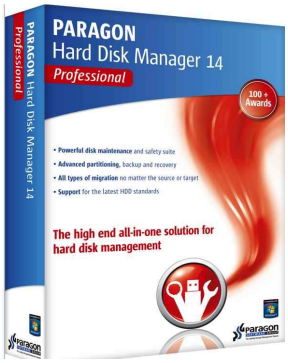
На 10-20% вырастет

<< спрос на дата-центры в России в начале 2015 года>>

ТЕХНОЛОГИИ. ОБОРУДОВАНИЕ. ПРОДУКТЫ. УСЛУГИ

Вышел Paragon Hard Disk Manager 14 для Hyper-V — бесплатное решение для СМБ

15 сентября 2014, Россия, Москва
Источник: centrlan.net



Компания Paragon Software Group (PSG), разработчик решений для резервного копирования, аварийного восстановления и миграции данных, выпустила Paragon Hard Disk Manager 14 для Hyper-V — новое бесплатное решение для ИТ-администраторов компаний малого и среднего бизнеса, которые ищут инструмент для осуществления полного спектра управленческих задач ИТ, в том числе обеспечения защиты виртуальных машин хоста Microsoft Hyper-V. В отличие от традиционных инструментов резервного копирования, предназначенных для работы с физическими машинами, новый продукт работает на уровне виртуализации для того, чтобы без использования сторонних агентов резервного копирования защитить любую гостевую машину Hyper-V: Hyper-V 2008, Hyper-V 2012 R1, Hyper-V 2012 R2 (Windows, Linux и т.д.), сообщили CNews в Paragon.

По словам представителей компании, защита виртуальных машин без агента позволяет оптимизировать процесс резервного копирования данных, минимизируя загрузку хоста и гипервизора в течение всего процесса. Paragon Hard Disk Manager 14 для Hyper-V предлагает широкий выбор форматов резервного копирования, в том числе в виртуальный контейнер pVHD (Paragon Virtual Hard Drive), который настроен по умолчанию и впоследствии может быть изменен на VMDK, VHD или VHDX. При использовании VHD / VHDX в качестве целевого формата пользователь может подключить образ резервной копии к существующей виртуальной машине Hyper-V, и ОС будет успешно запущена. При использовании pVHD появляются дополнительные опции: сжатие высокого уровня, шифрование или разбивка файла образа виртуальной машины. Продукт позволяет сделать резервную копию гостевой машины Hyper-V непосредственно в виртуальный контейнер других гипервизоров (VMware или Oracle), что упрощает процесс V2V-миграции с Hyper-V, отметили в Paragon.

Делая резервную копию в формате pVHD (виртуальный жесткий диск Paragon), пользователь может сократить объем занимаемого места в резервном хранилище и предотвратить несанкционированный доступ к персональным данным благодаря шифрованию по стандарту AES (расширенный стандарт шифрования). Для поддержки внешних хостов с их собственными гостевыми машинами компания предлагает предприятиям среднего и крупного бизнеса использовать более мощное решение — Paragon Protect & Restore.

Среди ключевых возможностей Paragon HardDisk Manager 14 для Hyper-V: интегрированный Microsoft VSS — создание архива виртуальной машины Hyper-V в режиме реального времени с помощью Microsoft Hyper-V VSS Writer и без использования стороннего агента резервного копирования; защита гостевой машины Hyper-V — возможность резервного копирования целых виртуальных машин, работающих под управлением Hyper-V или просто находящихся на хосте Hyper-V; гранулярное восстановление данных из архива Hyper-V — возможность восстановления только необходимых файлов, без восстановления полного образа виртуальной машины; восстановление гостевой машины Hyper-V — возможность восстановления резервной копии виртуальной машины из наиболее подходящей «точки восстановления», отражающей состояние виртуальной машины на определенный момент времени; широкий спектр операций по управлению жесткими дисками и разделами — позволяет виртуальным машинам работать на полную мощность (MFT-дефрагментация, подключение виртуальных дисков, изменение размера кластера, слияния / разделения разделов и т.д.).

Больше функций для работы с разделами и данными на жестком диске доступны в Paragon Protect & Restore.

Paragon Hard Disk Manager 14 для Hyper-V может быть установлен на Windows 8.1, Server 2008 R2, Server 2012 R1 и Server 2012 R2 с Hyper-V ролью для защиты гостевых машин, поддерживаемых Hyper-V. Решение доступно для бесплатного скачивания всем представителям малого и среднего бизнеса.

Компания "Аладдин Р.Д." представила новейшие технологии в сфере обеспечения информационной безопасности в корпоративной мобильной инфраструктуре

15 сентября 2014, Россия, Москва
Источник: press-release.ru

Сергей Груздев, генеральный директор "Аладдин Р.Д.

Компания "Аладдин Р.Д.", ведущий российский разработчик и поставщик решений для обеспечения информационной безопасности, приняла участие во втором ежегодном Форуме "Samsung Enterprise Mobility Forum", прошедшем 11 сентября в Москве.

В рамках Форума участники мероприятия обсудили вопросы, касающиеся корпоративной мобильности, в том числе лучшие бизнес-практики от лидеров рынка, обеспечения информационной безопасности в мобильной инфраструктуре, а также рассмотрели аппаратные и программные решения компании Samsung.

На тематической секции, посвящённой информационной безопасности, с докладом "ИБ в корпоративной мобильной инфраструктуре" выступил генеральный директор "Аладдин Р.Д." Сергей Груздев. В ходе выступления спикер рассказал о новейших технологиях, обеспечивающих возможность использования мобильного телефона для формирования усиленной квалифицированной электронной подписи и строгой двухфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам.

Одной из основных сложностей, возникающих при построении политики информационной безопасности мобильной инфраструктуры компании, является неудобство использования корпоративных электронных ключей и смарт-карт для мобильных устройств в силу того, что разъёмы смартфонов не унифицированы, для подключения к ним необходимы различные виды токенов и переходников. Решением данной проблемы может стать применение технологии "ЭП на SIM-карте", благодаря которой само мобильное устройство может использоваться в качестве токена безопасности, позволяющего формировать персональную ЭП, визуализировать подписываемые документы и безопасно вводить PIN-код.

Уникальность данного решения заключается в том, что технология "ЭП на SIM-карте" может работать как с помощью онлайн-каналов (SMS от оператора связи), так и с применением оффлайн-технологий (NFC). Таким образом, даже при отсутствии мобильной связи пользователь мобильного телефона, применяющий данное решение, сможет подписать электронный документ или авторизоваться в системе.

После оживлённой дискуссии, последовавшей за выступлением эксперта "Аладдин Р.Д.", участники мероприятия пришли к выводу, что представленная в рамках доклада технология позволит существенно расширить не только перечень российских компаний, поддерживающих концепцию BYOD, но и список электронных сервисов и услуг, предназначенных для физических лиц.

"Аладдин Р.Д." – ведущий российский разработчик и поставщик продуктов и решений для обеспечения информационной безопасности. Компания специализируется на комплексном подходе к решению задач аутентификации и защиты персональных данных.

"Аладдин Р.Д." активно развивает свой бизнес в направлении разработки решений и оказании услуг для крупных корпоративных клиентов и государственного сектора. Это позволило ей войти в ТОП-3 крупнейших компаний России в сфере разработки аппаратного обеспечения для информационной безопасности по итогам рейтинга IDC, а также ТОП-100 крупнейших ИТ-компаний (рейтинг CNews Analytics, 2013), ТОП-50 крупнейших ИТ-разработчиков (рейтинг CNews Analytics, 2013) и ТОП-50 крупнейших поставщиков ИТ для банков (рейтинг CNews Analytics, 2013). Продукты компании и комплексные решения на их основе востребованы в различных секторах отечественной экономики, в том числе в банковском, государственно-административном, а также в ТЭК и ряде других.

Компания "Аладдин Р.Д." прошла сертификацию менеджмента качества на соответствие российским стандартам ГОСТ Р ИСО 9001-2011.

Лидерские позиции "Аладдин Р.Д." подкреплены 19-летним опытом работы на российском рынке информационной безопасности, а также прочными партнёрскими отношениями с ведущими российскими разработчиками систем криптографической защиты информации (СКЗИ), системными интеграторами и ведущими технологическими лидерами: Athena Smartcard Solutions, Microsoft, Oracle, Apple, VASCO, Gemalto и др.

ФБР запустило инновационную систему слежки за гражданами на улицах

16 сентября 2014, США
Источник: warandpeace.ru

В США в полную силу заработала новая система слежения за гражданами. Ее главная особенность: способность идентифицировать лица в толпе, используя камеры видеонаблюдения. К концу 2015 г. система будет содержать 52 млн изображений лиц людей, включая простых прохожих, не замешанных в каких-либо преступлениях.

Федеральное бюро расследований (ФБР) США завершило внедрение новой национальной системы идентификации Next Generation Identification (NGI) System. Об этом говорится в официальном сообщении.

Внедрение NGI System проходило в несколько этапов в течение трех с половиной лет. Первый этап был завершен в феврале 2011 г. Теперь же NGI System функционирует в полную силу.

Главная особенность новой системы заключается в ее способности выхватывать и идентифицировать лица из толпы, используя камеры видеонаблюдения. Агенты смогут обращаться к базе данных лиц и отслеживать перемещения людей вне зависимости, являются ли они подозреваемыми или простыми людьми, не замешанными в каких-либо преступлениях.

В течение последних трех с половиной лет проходило наполнение базы данных NGI System. В настоящее время она содержит 8 млн изображений лиц. К концу 2015 г. бюро рассчитывает расширить базу в 6,5 раз — до 52 млн фотографий.

База данных позволяет агентам узнавать, где в последний раз был замечен подозреваемый. Кроме того, специальная функция Rap Back позволит сотрудникам правоохранительных органов получать уведомления в режиме реального времени, содержащую информацию о перемещениях человека.

Неизбирательность NGI System — а именно тот факт, что система записывает в базу данных фотографии лиц всех людей подряд — была раскритикована рядом правозащитных организаций, включая Electronic Frontier Foundation. Сторонники права на частную жизнь подчеркнули, что в настоящий момент власти США даже не договорились, кто может иметь доступ к этой базе данных, а кто — нет.

Между тем, точность работы системы пока невысока. Если в нее загрузить фотографию человека, то она выдаст в ответ 50 снимков, на которых может быть также изображен этот человек. При этом вероятность, что его фотография будет в этом списке, составляет только 85%.

Помимо фотографий, NGI System содержит свыше 100 млн отпечатков пальцев и связанные с ними персональные данные — имя и фамилию, национальность, номер паспорта, возраст и домашний адрес.

Система CONTACT и портал Banki.ru запустили сервис идентификации пользователей

16 сентября 2014, Россия, Москва
Источник: press-release.ru

Таким образом можно получить онлайн-доступ к своей кредитной истории в личном кабинете на портале Banki.ru. Сервис также действует для портала Mycreditinfo.ru. Ранее идентификацию можно было пройти только в офисах Banki.ru и Mycreditinfo.ru, на Почте России и с помощью курьерской службы.

Теперь оперативно получить доступ к своей кредитной истории можно в шаговой доступности по всей России - новый способ идентификации доступен более чем в 1250 населенных пунктов.

Для прохождения идентификации через систему CONTACT необходимо:

- в разделе «Кредитные истории» на порталах Banki.ru или Mycreditinfo выбрать идентификацию при помощи системы CONTACT;

- обратиться в любой пункт системы CONTACT на территории РФ;

- сообщить операционисту о прохождении идентификации в адрес «Банки.ру-Технологии»;

- предъявить паспорт;

- оплатить 250 руб., из которых 100 руб. – сумма перевода на личный аккаунт и 150 руб. – сумма комиссии.

Идентификация и перечисление денежных средств происходят в режиме реального времени. То есть сразу же после прохождения процедуры пользователь может заказать и моментально получить свою кредитную историю в личном кабинете на порталах Banki.ru или Mycreditinfo.ru.

Напомним, что идентификация пользователей как заемщиков необходима для доступа к кредитной истории согласно требованиям федеральных законов 152 «О защите персональных данных» и ?218 «О кредитной истории». При этом пользователю порталов Banki.ru и Mycreditinfo.ru достаточно пройти эту процедуру один раз, чтобы затем иметь постоянный доступ к своей кредитной истории в личном кабинете.

«Мы не только помогаем посетителям Банки.ру управлять личными финансами, но и стремимся предоставить для этого удобный функционал, — рассказывает генеральный директор Банки.ру Филипп Ильин-Адаев. — С появлением оперативного способа идентификации еще большее количество наших пользователей сможет следить за своей кредитной историей онлайн, как это принято во многих развитых странах мира».

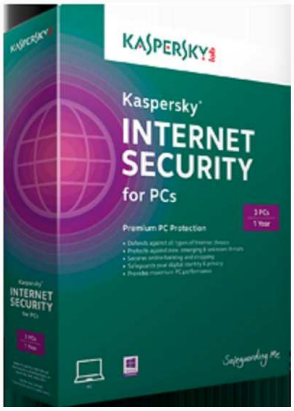
КОМПЕТЕНТНОЕ МНЕНИЕ:

Раиса Назмутдинова, CONTACT, директор департамента развития и управления продуктами

<<Проекты портала Банки.ру позволяют миллионам пользователей управлять информацией, полученной на ресурсе. Запуск нашего совместного сервиса по идентификации пользователей даст возможность клиентам осуществлять контроль за своей кредитной историей и знать ее оценку со стороны банков и БКИ. Наши партнерские отношения с порталом Банки.ру - это дополнительный импульс к развитию новых проектов, а широкий географический охват CONTACT - возможность открыть доступ к кредитным историям еще большему числу жителей России.>>

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 тех-

нологии 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.

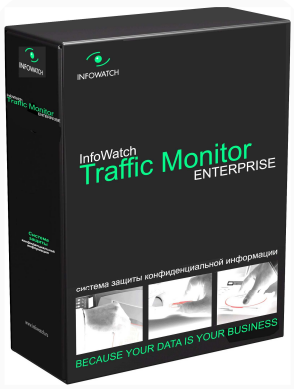
По информации «Рамэк», Safe обеспечивает разграничение доступа по средствам двухфакторной аутентификации пользователя, возможность аудита событий, выполнение требования ФЗ №152 «О персональных данных». Защищенные рабочие станции Ramec Safe будут полезны всем компаниям, выполняющим обработку персональных 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.

Trend Micro представила ПО для снижения числа уязвимостей

25 сентября 2014, Япония
Источник: pcweek.ru

Trend Micro Security 2015

Компания Trend Micro Incorporated, глобальный разработчик программного обеспечения в области информационной безопасности, выпустила наиболее полное решение, предлагающее защиту от киберугроз для PC, Mac, Android и для платформы iOS. Trend Micro Security 2015 — это решение класса «все в одном», помогающее предотвращать проблемы с безопасностью и конфиденциальностью, которые преследуют пользователей Интернета.

Недавнее исследование, проведенное по заказу Trend Micro, показало, что интернет-пользователи совершают различные потенциально рискованные действия, просматривают подозрительные сайты и разрешают приложениям получать доступ к публичной информации из своих профилей в социальных сетях. Например, 67 процентов респондентов позволяют браузерам сохранять свои пароли при работе в Интернете. Поскольку учетные записи мобильных устройств все чаще являются общими с учетными записями домашних компьютерных сетей, Trend Micro разработала комплексное решение для обеспечения безопасности, которое гарантирует защиту пользователя независимо от того, какое устройство он использует в данный момент.

Такие решения, как Trend Micro Security 2015, сегодня необходимы как никогда, о чем свидетельствуют результаты исследования, показавшего, что рискованное поведение интернет-пользователей создало

новые возможности для атак киберпреступников. Вот некоторые результаты исследования: 40 процентов пользователей не применяют пароли для защиты своих мобильных устройств; 28 процентов респондентов разрешают мобильным приложениям получать доступ к своим профилям в социальных сетях; 10 процентов пользователей мобильных устройств предполагают, что загрузили вредоносное приложение на свое устройство.

Trend Micro Security 2015 помогает защитить интернет-пользователей от потенциально опасной онлайн-активности. Это решение обеспечивает лучшую в отрасли защиту от вирусов и веб-угроз, идентифицируя и блокируя опасные ссылки на веб-сайтах, в социальных сетях, электронной почте и службах обмена мгновенными сообщениями. Оно также обнаруживает спам, содержащий «фишинг» — мошеннические уловки, которые могут заставить пользователей раскрыть свою конфиденциальную персональную информацию.

Кроме того, компания Trend Micro выяснила, что более двух третей пользователей Интернета позволяют своим браузерам сохранять пароли онлайн, что является опасной практикой, допускающей возможность взлома, особенно в свете недавних нарушений конфиденциальности данных в сфере розничной торговли. Чтобы помочь бороться с кражами паролей и личных данных, Trend Micro Security 2015 включает диспетчер паролей, который шифрует все онлайн-пароли, позволяя пользователям легко заходить на веб-сайты, не опасаясь кражи паролей.

Диспетчер паролей также работает на нескольких устройствах и предоставляет генератор паролей, чтобы предотвратить общепринятую, но небезопасную практику использования одного и того же пароля для нескольких учетных записей.

С целью обеспечения конфиденциальности и безопасности пользователей Интернета в Trend Micro Security 2015 расширены возможности сканера конфиденциальности социальных сетей: помимо Facebook, Twitter и Google+ он сканирует еще и LinkedIn. Теперь пользователи могут полностью положиться на технологии компании Trend Micro, помогающие сохранить конфиденциальность, безопасность и положительную сетевую репутацию. Согласно результатам исследования Trend Micro, интернет-пользователи по-прежнему совершают действия, повышающие риск кражи их личных данных или нанесения ущерба их репутации. Вот краткий обзор некоторых из этих результатов: 74 процента интернет-пользователей отметили, что они обеспокоены необходимостью делиться персональными данными через социальные сети; 60 процентов пользователей социальных сетей удаляли свои публикации, опасаясь последствий в личной жизни; 40 процентов сообщили, что делятся результатами своих игр в социальных сетях; у 11 процентов в «друзьях» в социальной сети были их начальники.

КОМПЕТЕНТНОЕ МНЕНИЕ:
Акихико Омикава, Trend Micro, генеральный менеджер

<<Trend Micro Security 2015 обеспечивает защиту от угроз и конфиденциальность независимо от устройства или операционной системы. Это решение защищает персональную информацию от раскрытия киберпреступниками, обеспечивает конфиденциальность и защищает при работе в Интернете. Первый шаг к защите нашей цифровой жизни — всегда помнить о тех опасностях, которые представляет Интернет для конфиденциальности и персональных данных. Каждый из нас является потенциальной мишенью для киберпреступников, однако Trend Micro Security 2015 защищает пользователя в любое время, в любом месте и на любом устройстве, действуя как эффективное средство сдерживания угроз.
Смартфоны и ноутбуки являются нашими постоянными спутниками, однако управление конфиденциальностью и безопасностью в этом все более „цифровом" мире часто упускается из виду. Чтобы уменьшить беспокойство интернет-пользователей в отношении конфиденциальности и излишней откровенности, Trend Micro Security 2015 позволяет им сохранять конфиденциальность в Интернете, защищая их данные от посторонних лиц и киберпреступников.>>

Рекламная сеть Facebook научилась отслеживать людей при смене устройств интернет-доступа

29 сентября 2014, США
Источник: internet.cnews.ru

Новая платформа Facebook не только делает мобильную рекламу эффективнее, но и несет новые вопросы, связанные с безопасностью персональных данных. Особенность продукта заключается в способности отслеживать конкретных людей по мере того, как они переходят от одного устройства к другому для выхода в интернет.

Социальная сеть Facebook объявила о запуске рекламной платформы Atlas, призванной усилить конкуренцию с лидером рынка онлайн-рекламы - компанией Google.

Платформа Atlas существовала ранее и принадлежала Microsoft до тех пор пока в феврале 2013 г. ее не приобрела Facebook. С тех пор инженеры крупнейшей в мире соцсети занимались ее модернизацией и в итоге переделали платформу практически полностью, с нуля переписав ее код.

Особенность Atlas, на которой Facebook многократно сделала акцент на презентации в Нью-Йорке и на официальном сайте, заключается в «человеко-ориентированности». Во всем потоке декстопного и мобильного трафика Atlas следит за поведением конкретного человека. То есть если, например, пользователь нашел какой-то товар в интернете с помощью мобильного телефона и затем сел за ноутбук, чтобы его купить, для платформы это будет один и тот же человек, хотя и обезличенный.

«Atlas предлагает человеко-ориентированный маркетинг, помогая рекламодателям достигать потребителей вне зависимости от устройства, платформы и издателя», — рассказал глава Atlas Эрик Джонсон (Erik Johnson).

Проблема современного интернет-маркетинга, утверждают в Facebook, в отсутствии возможности задействовать те же механизмы таргетинга на мобильных устройствах, что и на настольных ПК. В частности, речь идет о куках (cookies) — фрагментах данных, которые создаются на локальном устройстве удаленным сервером и служат для хранения статистики и предпочтений пользователя.

«На мобильных устройствах куки не работают. Поэтому продавать таргетированную рекламу сложнее. И непросто определить, был ли в конечном счете товар приобретен, так как для покупки пользователь может воспользоваться другим устройством», — пояснил Джонсон. Atlas, по его словам, лишена этого недостатка, так как цепляется за человека, с какого бы устройства он ни выходил в сеть.

<<...С запуском Atlas в новом формате, будучи второй по величине игрок рынка интернет-рекламы Facebook сможет усилить конкуренцию с занимающей лидирующую позицию Google...>>

В компании не раскрывают информацию о том, как именно они отслеживают потребителя. Как пишет Wall Street Journal, при каком-либо акте взаимодействия пользователя с рекламой, размещенной в сети Atlas, данные об этом взаимодействии отправляются в аккаунт пользователя на Facebook. Таким образом, аккаунт в Facebook служит связующим звеном при использовании устройств различного типа.

В Facebook уверены, что особенность Atlas увеличит мировые расходы на мобильную рекламу. «Платформа изменит рынок мобильной рекламы, — приводит слова представителя Facebook газета WSJ. — Потребители стали проводить больше времени за мобильными устройствами, нежели за десктопами. Но рекламодатели не спешат тратить на мобильную рекламу из-за отсутствия механизмов таргетинга. Теперь этому сегменту развиваться ничто мешать не будет».

Помимо кросс-платформенности, Atlas был наделен полностью новым интерфейсом и расширенными аналитическими инструментами.

Первым клиентом Facebook, согласившимся использовать платформу Atlas, стало рекламное бюро Omnicom, обслуживающее свыше 5 тыс. клиентов во всем мире, включая известные мировые бренды.

С запуском Atlas в новом формате, будучи второй по величине игрок рынка интернет-рекламы Facebook сможет усилить конкуренцию с занимающей лидирующую позицию Google. По данным eMarketer, компании Facebook принадлежит 6% мирового рынка интернет-рекламы, включая мобильную рекламу. Тогда как Google - 32%. В то же время новая платформа рождает новые вопросы, связанные с безопасностью персональных данных: что именно о пользователе будет собирать Facebook и насколько надежно сможет хранить эти сведения?

В 2013 г., согласно eMarketer, Google занял 41,5% мирового рынка мобильной рекламы, при этом по сравнению с 2012 г. его доля сократилась (в 2012 г. — 49,8%). Доля Facebook в прошлом году составила около 16%, увеличившись почти вдвое (с 9%) по сравнению с 2012 г.

Персональные данные военнослужащих защитит износостойкий пластик

29 сентября 2014, Россия, Башкортостан респ.
Источник: bashinform.ru

Персональные электронные карты (ПЭК)

Износостойкий поликарбонат, из которого изготавливаются персональные электронные карты военнослужащих, позволит обеспечить надёжную сохранность удостоверения от повреждений и внешних воздействий в ходе боевой подготовки и повседневной деятельности солдат и офицеров, сообщили в пресс-службе Центрального военного округа.

Материал обеспечит защиту электронных данных при температуре эксплуатации от минус 40 до плюс 100 градусов по Цельсию при сроке службы карты в 10 лет. Информация о военнослужащем содержится в памяти встроенного микроконтроллера объёмом 160 Кб. Этого достаточно для хранения 59 различных параметров о состоянии здоровья, физическом развитии, морально-психологических и деловых качествах,

профессиональной подготовке, образовании, семейном положении.

Персональные электронные карты будут использоваться в различных автоматизированных системах военного назначения в ходе службы и при увольнении в запас.

Персональные электронные карты (ПЭК) начали выдаваться российским военнослужащим в ходе весеннего призыва с 1 апреля 2014 года. В них содержится фотография призывника, указываются демографические данные, медицинские показатели и решение о месте прохождения военной службы, сведения о профессиональной подготовке новобранца. В Минобороны РФ уверены, что ПЭК позволит упростить систему назначения на воинские должности и облегчит ведение воинского учета граждан. Формирование персональных данных будет проходить только на специальных комплексах средств автоматизации, что исключит попытку их взлома и попадание материалов в интернет.

Softline представила новый IaaS-продукт на базе Microsoft Windows Azure Pack

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

Компания Softline запустила хостинговое решение на базе Microsoft Windows Azure Pack в собственном «облаке». Теперь клиенты компании смогут получить высокотехнологичную услугу по размещению ИТ-приложений, высоконагруженных веб-сайтов, баз данных, сообщили CNews в Softline.

Windows Azure Pack — это решение для Windows Server и System Center. Оно позволяет провайдерам и заказчикам работать в собственном ЦОДе с сервисами, основанными на тех же технологиях, что и в публичном «облаке» Windows Azure: портал управления, сервисы для хостинга сайтов и виртуальных машин. Однако Azure Pack инсталлируется в инфраструктуре провайдера. Таким образом, интерфейс внешне практически ничем не отличается от Windows Azure и дает возможность реализовать самообслуживание и многозадачность как на уровне IaaS, так и на уровне PaaS на мощностях сервис-провайдера, расположенных на территории России, пояснили в компании.

Технология позволяет быстро и легко осуществлять миграцию физических и виртуальных серверов в «облако», мощность которого не ограничена и располагает ресурсами под любые проекты. При этом аппаратная часть ИТ-инфраструктуры заказчика недоступна для других облачных пользователей. Управление виртуальным дата-центром происходит с помощью веб-портала. «Облако» Softline безопасно: для построения технологичной платформы используются дата-центры не ниже уровня Tier-3, осуществляется контроль физического доступа к размещенному оборудованию, используются шифрованные каналы связи и разграничение доступа, подчеркнули в компании.

Возможности Windows Azure Pack делают продукт востребованным у компаний не только СМБ-сектора, для бизнеса которых важно настроить стандартные сервисы в виде облачной почты, портала, службы каталогов Active Directory, терминального доступа. Он интересен будет и для заказчиков Enterprise-уровня, считают в Softline. Удобный интерфейс, единое окно управления для гибридных систем, простой и понятный функционал, а также возможность гибко управлять облачными ресурсами позволяют экономить время и деньги крупных компаний при расширении текущих проектов и запуске новых.

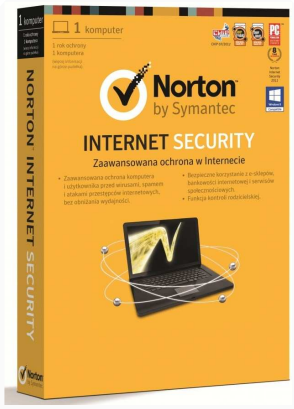
Данный сервис также удобен для разработчиков ПО — платформа обладает широким функционалом автоматизации. Помимо шаблонов виртуальных машин, доступны их роли из галереи, которые позволяют сократить до минимума время на развертывание типовых сервисов инфраструктуры.

В связи с новыми поправками в законодательство по защите персональных данных клиенты, использующие сейчас Microsoft Azure (Ирландия), могут безболезненно перейти на сервис Softline, поскольку они смогут и дальше использовать привычный интерфейс управления, но при этом решат проблему, связанную с хранением данных на территории России, подчеркнули в компании.

«Клиент получает панель управления, которая внешне и функционально аналогична Microsoft Azure. Отличительной ее особенностью являются возможности по созданию гибридных "облаков": часть инфраструктуры находится в "облаке" Softline в России, часть — в Microsoft Azure, а часть — на собственных серверах в организации (при использовании виртуализации от Microsoft). Все данные из различных ресурсов вне зависимости от их расположения можно свести в единую панель управления, а виртуальную машину — переносить из одного сегмента в другой. Использование ИТ-инфраструктуры облачных провайдеров позволяет клиентам поручить необходимую поддержку и обслуживание и сократить расходы на ее содержание», — рассказал Леонид Аникин, руководитель направления облачной ИТ-инфраструктуры компании Softline.

Мощная защита от угроз — в новом решении Norton Security

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



антивирусное ПО Norton

В стремлении объединить девять основных продуктов в одно флагманское решение, компания Symantec объявила о выпуске "Norton Security". Это новое решение обеспечивает многоуровневую защиту всех устройств пользователя от сложных и эволюционирующих угроз на всех платформах. "Norton Security" также предлагается и с функцией встроенного резервного копирования, что защитит пользователей от потерь их наиболее важных файлов данных, фотографий и контактов.

По данным «Отчёта об угрозах безопасности в интернете за 2014 год» компании Symantec, количество направленных атак на персональные данные возросло за прошлый год на 91%, и более 550 миллионов человек стали их жертвами. Для пользователей становится всё более важным вопрос защиты себя в этом очень сложном и пронизанном технологиями мире, вне зависимости от используемых ими устройств. "Norton Security" является высокоэффективным и очень простым в использовании решением на основе передовых технологий и аналитических данных компании Symantec, которое поможет пользователям защититься от современных кибер-угроз.

Новый Norton "Norton Security" – это единое решение, спроектированное для защиты PC и Mac, а также смартфонов и планшетов на платформах Android и iOS. Основные характеристики и возможности "Norton Security" включают в себя:

Лучшие в своём классе производительность и защита: по данным тестов, проведённых тремя независимыми организациями в сентябре 2014 года, "Norton Security" – это не только самый быстрый продукт защиты, но он также набрал 100% в категории «время обеспечения защиты» ("time-to-protect"), блокировав все вредоносные атаки в первый же день; и набрал 100% в категории «Защита от уязвимостей».

Не только антивирус: "Norton Security" создан на запатентованных инновационных технологиях, таких как: Insight, SONAR и мониторинг угроз с агрессивными эвристическими методами обнаружения, позволяющими выявлять даже самые стойкие из них. Более того, Safe Web, Scam Insight, Download Insight и технологии защиты от фишинга обмениваются друг с другом информацией для выявления сайтов, используемых мошенниками для новых социально-инжиниринговых атак.

100% гарантия отсутствия вирусов: мы настолько уверены в нашей защите от вирусов и вредоносных программ, что вернём деньги, если "Norton Security" и эксперты Norton не смогут удалить вирус с PC или Mac.

Управление программой важно так же, как и защита: решение "Norton Security" разработано с нуля, чтобы сделать для пользователей простыми, чем когда-либо ранее, установку и управление их защитой через облачный Web-портал. Обновлённый интерфейс портала позволяет максимально просто защищать новые устройства, отслеживать состояние защиты и управлять параметрами подписки.

<<...Количество направленных атак на персональные данные возросло за прошлый год на 91%, и более 550 миллионов человек стали их жертвами...>>

Защищённое хранилище Identity Safe – это защищённое хранилище, которое запоминает, надёжно хранит и автоматически вводит логины и пароли на соответствующих порталах и сайтах. В условиях постоянно растущего количества инцидентов, связанных с кражей паролей и последующей утечкой информации, Identity Safe поможет сохранить логины и пароли от потери или кражи.

Аналитическая оценка мобильных приложений: Norton Mobile Insight отслеживает более 200 магазинов мобильных приложений по всему миру, осуществляя динамический анализ поведения предлагаемых ими приложений. Это позволяет защититься от программ, ворующих персональную информацию с устройств, изменяющих настройки, размещающих рекламу в панели уведомлений и требующих большего расхода батареи или передачи больших объёмов данных. Благодаря такой информации, потребители лучше понимают какая персональная информация собирается и передаётся, и почему растут расходы на передачу данных.

Резервное копирование наиболее ценных файлов и изображений: пользователям предоставляется возможность покупки "Norton Security" с 25 ГБ облачного хранилища для резервного копирования личных файлов, изображений, видео и любых других важных данных.

Глобальное отслеживание угроз и бесплатная техническая поддержка: "Norton Security" обслуживает команда из более 500 экспертов, распределённых по всему миру, ответственных за защиту пользователей от современных угроз. Она использует в своей работе более 41,5 млн. датчиков атак, регистрирующих тысячи событий в секунду в более чем 157 странах мира.

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).

Microsoft анонсировала Windows 10

01 октября 2014, США
Источник: sotovik.ru

Всем предположениям и слухам, как же Microsoft назовет очередной масштабный выпуск настольный платформы, наступил конец. Считалось, что компания Билла Гейтса выберет для апдейта, проходящего код кодовым обозначением Windows Threshold, такие маркетинговые имена, как Windows 9, Windows 365, Windows TH, Windows X или Windows One, однако было решено остановиться на Windows 10.

Идея и амбиции Windows 10 столь сильно отличаются от прежних Microsoft-систем, что наращивать номер версии до «девятки» было бы неверным, вот почему в Редмонде решили его перескочить.

Windows 10, подаваемая Microsoft «самой всесторонней платформой», предложит унифицированный пользовательский интерфейс Universal и способы взаимодействия с ним, одинаковые на любом совместимом оборудовании. Ну а разработчики приложений смогут создавать универсальные программы, выставляемые в едином магазине и умеющие запускаться на всех поддерживаемых вычислительных устройствах. Все последующие обновления платформы будут идти под стягом именно Windows 10 — похоже, подход Apple в сохранении Mac-системы в рамках OS X с номерами версий в формате 10.x не дает Редмонду покоя.

«Windows 10 будет работать на невероятно широком спектре девайсов: от Интернета вещей, смартфонов и планшетов до персональных компьютеров, игровой консоли Xbox и серверов в центрах обработки данных предприятия. Некоторые из таких устройств будут располагать крошечным 4-дюймовым экраном, другие опираться на огромные 80-дюймовые панели, а третьи вообще идти без дисплеев. Одни аппараты лежат в руках, вторые находятся на расстоянии нескольких метров. Управление Windows 10

ведется равно как через сенсорные прикосновения и стилус, так и мышь, клавиатуру, геймпад, жесты, притом что между указанными контроллерами легко переключаться».

Когда всё собирается вместе, речь, кажется, идет о чем-то, похожем на Windows 7, и сделано это намеренно. Джо Бельфиор, корпоративный вице-президент подразделения операционных систем, указал на миллионы клиентов Microsoft, всё еще обращающихся к Windows 7. Для таких пользователей было бы здорово обрести путь безболезненного перехода на Windows 10 в отличие от спорных концепций Windows 8, дебютировавшей осенью 2012 года.

«Нам бы хотелось сформировать такое ощущение, будто пользователи вчерашней Windows 7 сидели за рулем „Приуса", а сегодня едут в „Тесле", за которой скрывается Windows 10».

По словам Терри Майерсона, исполнительного вице-президента подразделения операционных систем, «Windows 10 предложит верный путь обращения с правильным устройством в корректное время». Вот почему следует надеяться на гибкий пользовательский интерфейс, адаптирующийся под оборудование, на котором запускается Windows 10. Это означает, что система знает, как видоизменить и подстроить, к примеру, Word или OneDrive под специфику окружений тех же планшетов или ноутбуков, дабы владелец извлекал максимум преимуществ того или иного устройства.

В общем и целом новинка сочетает лучшие элементы и наработки хорошо знакомой Windows 7, на сегодня самой популярной настольной операционной системы, с функциональностью Windows 8, привносящей новизну в привычный всем проект.

Так, меню «Пуск» Windows 10 смешивает классику этой кнопки в правом нижнем углу Windows 7 и новации стартового экрана Metro в составе Windows 8. От первой остался прокручивающийся список установленных в системе приложений, второй принес прикрепляющиеся «живые» плитки, причем с переменным размером. Другими словами, речь идет об обогащении «Пуск» фактически виджетами.

В «Пуске» появился универсальный поиск, объединяющий результаты, найденные на локальном устройстве и в Вебе.

Вся панель «Пуска» поддерживает изменение собственных размеров в любых масштабах, ограниченных лишь площадью экрана.

<<...Windows 10 избавлена от дуализма нынешней Windows 8, когда в одной среде сосуществуют традиционные приложения «Рабочего стола» и модные программы Metro, или Modern...>>

Windows 10 избавлена от дуализма нынешней Windows 8, когда в одной среде сосуществуют традиционные приложения «Рабочего стола» и модные программы Metro, или Modern. Софтверное наполнение причесано одним гребнем.

Подсистема многозадачности Windows 10 преобразилась, став гораздо удобнее в эксплуатации, хотя и изрядно напоминает Mission Control в OS X. Отныне она доступна тремя способами: традиционной комбинацией клавиш Alt + Tab, жестом смахивания влево, новой кнопкой на панели задач.

На одном экране можно одновременно вывести окна четырех приложений, что, несомненно, упростит параллельную работу.

Внедрены рабочие пространства: множество виртуальных рабочих столов с запущенными наборами приложений на каждом из них.

Microsoft, понимающая ущербность Windows 8 в ее исключительном фокусе на сенсорном управлении, всё же не стала лишать Windows 10 поддержки последнего, потому панель Charms осталась на месте, пройдя череду улучшений.

Для устройств-трансформеров типа Lenovo Yoga 2 Pro пригодится новый подход Continuum, нужный для бесшовного переключения между режимами клавиатурного лэптопа и сенсорного планшета.

Командная строка наконец-то (!) научилась воспринимать клавиатурные команды выделения, копирования и вставки.

Для корпоративного сектора, самого важного для бизнеса Microsoft, Windows 10 сделала акцент на четырех вещах: хорошо приспособленная среда для обновлений, современные инструменты управления устройствами, включая мобильные, — Active Directory, Group Policy и MDM, фирменная настройка магазина Windows Store для внутренних приложений, защита и разделение рабочих и личных данных.

«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 об-

лачного 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).

Челябинский студент изобрел программу по защите персональных данных

02 октября 2014, Россия, Челябинская обл.
Источник: chel.kp.ru

Пароли невозможно подсмотреть и запомнить.

Приложение Bloolocker выпустили год назад. Оно является итогом дипломной работы студента ЧелГУ Александра Бутакова.

— Мы хотели сделать программу для "андроида" устойчивой к подглядыванию через плечо. Пользователь больше не должен запоминать длинные пароли, использовать простые и ненадежные. — рассказал Александр. — Вместо них теперь будет использоваться сотовый телефон. Защита будет действовать через bluetooth. Имея при себе мобильник и находясь рядом с компьютером, человек может свободно пользоваться ПК. Но стоит убрать устройство из зоны действия bluetooth — компьютер автоматически включает блокировку. То есть, пользоваться им уже невозможно.

Программа защиты студента ЧелГУ не имеет аналогов. Несмотря на противоречивые отзывы, проект завоевывает интерес аудитории.

ИНДИКАТОРЫ РАЗВИТИЯ. ОБЗОРЫ. АНАЛИТИКА

Российская практика

49% пользователей боятся публикации своей переписки

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

Не менее 3/4 россиян скрывают те или иные детали своей активности в интернете. К этому выводу пришла международная антивирусная компания ESET (Словакия) в результате опроса пользователей.

Участникам опроса было предложено выбрать один вариант ответа на вопрос: «Какую сторону вашей сетевой жизни вы бы не хотели обнародовать ни при каких обстоятельствах?».

Большинство респондентов (49%) опасаются рассекретить личные сообщения в социальных сетях, онлайн-мессенджерах или электронной почте.

Второй по популярности вариант ответа – «история поисковых запросов». Ее публикации опасаются 14% опрошенных.

У 9% участников опроса есть фотографии в «закрытых» альбомах в социальных сетях. Эти снимки они не хотели бы увидеть в общем доступе.

Наименее секретной информацией респонденты считают историю своих покупок в онлайн-магазинах (4%), а также списки друзей в социальных сетях (2%).

При этом почти четверть российских пользователей не боятся публикации данных о своей сетевой жизни. 22% участников опроса сообщили, что у них вообще нет секретов.

«Все предельно просто – чем меньше информации о себе вы оставляете в сети, тем меньше шансов на то, что нежелательные сведения попадут в открытый доступ, – комментирует Алексей Оськин, руководитель отдела технического и маркетингового сопровождения ESET Russia. – Если вы активно общаетесь онлайн, регулярно проверяйте настройки конфиденциальности аккаунтов в соцсетях, освобождайте почтовые ящики от старых писем и используйте сложные неповторяющиеся пароли для всех веб-сервисов».

Опрос ESET проходил в августе-сентябре 2014 года. В нем приняли участие более 1000 подписчиков официальных групп ESET Russia в социальных сетях и пользователей портала «Мы ESET».

Итоги конференции "Код информационной безопасности 2014"

11 сентября 2014, Россия, Москва
Источник: club.cnews.ru

Алексей Лукацкий – бизнес-консультант по безопасности Cisco

2014 год стал особым для конференции «Код информационной безопасности». Ровно 10 лет назад, в далеком 2005 году конференция прошла впервые, став одним из первых проектов агентства бизнес-событий «Экспо-Линк».

Тогда конференция представляла собой всего один поток из вереницы докладов, следующих один за другим. Что же «Код ИБ» представляет собой сейчас?

На конференции в 2014 году выступило более 20 спикеров и бизнес-тренеров. Мы разделили потоки «Кода Иб», основываясь на разнице в тематиках и форматах и постарались, чтобы каждый участник смог посетить все, интересные для него, выступления.

Фасилитационная секция.

Фасилитация — это профессиональная организация процесса групповой работы, направленная на прояснение и достижение группой поставленных целей. Процесс фасилитации приводит к повышению эффективности групповой работы, вовлеченности и заинтересованности участников, раскрытию их потенциала.

Для проведения фасилитационной секции мы специально пригласили Татьяну Куковякину – профессионального бизнес-тренера с 18-летним опытом проведения тренингов, с образованием в США и Великобритании за плечами, 10-летним управленческим опытом в сфере ИТ и титулами «Золотой дилер России», «Дилер десятилетия», «Женщина-предприниматель года” и др. Мастер класс Алексея Лукацкого

Впервые в рамках «Кода информационной безопасности» прошел полноформатный мастер-класс. Ведущим выступил Алексей Лукацкий – бизнес-консультант по безопасности ИТ-гиганта Cisco, по совместительству – автор одного из наипопулярнейших российских блогов по информационной безопасности и №1 в списке лучших ИБ-экспертов по версии Biz-Expert.

Алексей осветил вопрос применения и загвоздок закона о защите персональных данных как с юридической, так и с технической сторон. Участники посмотрели на динамику изменения закона за последние 8 лет и обсудили его преимущества, недостатки и даже способы обхода.

Как бухгалтеру избежать штрафа за нарушения при работе с персональными данными

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

Штрафы и проверки

На первый взгляд, штрафы за нарушение правил работы с персональными данными не так уж и высоки. Согласно статье 13.11 КоАП РФ штрафы составляют 5-10 тысяч рублей для организации и 500-1000 рублей для ее должностного лица.

Однако надо учитывать, что этот штраф может налагаться за каждое допущенное нарушение. А правил для тех, кто работает с персональными данными, законодатели установили очень много.

Кроме того, если в компании не утверждено Положение о персональных данных, то возможно наступление административной ответственности за нарушение трудового законодательства по статье 5.27 КоАП РФ. Штраф

может составить от 30 до 50 тыс. рублей. Также возможно административное приостановление деятельности на срок до девяноста суток. Кстати, с 2015 года штраф за повторное нарушение, предусмотренное данной статьей, составит уже от 50 до 70 тыс. рублей.

Соблюдение законодательства о персональных данных контролирует Роскомнадзор. За невыполнение предписания Роскомнадзора об устранении нарушений законодательства о персональных данных возможен административный штраф до 20 000 рублей (статья 19.5 КоАП РФ). Если же просто не ответить на запрос этого органа касательно персональных данных, то штраф может составить до 5 000 рублей (статья 19.7 КоАП РФ).

Ответственность работника

Работник, по вине которого было допущено нарушение норм, регулирующих обработку и защиту персональных данных других работников, может быть привлечен (статья 90 ТК РФ):

- к административной ответственности
- к дисциплинарной и материальной ответственности;
- к гражданско-правовой ответственности;
- к уголовной ответственности.

<<...Сэкономить время и сосредоточиться на своей основной работе можно с помощью веб-сервиса «Персональные данные»...>>

Административная ответственность

Персональные данные относятся к информации, доступ к которой ограничен. Поэтому за разглашение персональных данных ответственный работник может быть оштрафован на сумму от 4 до 5 тыс. рублей (статья 13.14 КоАП РФ «Разглашение информации с ограниченным доступом»).

Должностных лиц также можно привлечь к ответственности и за отсутствие утвержденного Положения о персональных данных. В этом случае штраф за нарушение трудового законодательства составит от 1 до 5 тыс. рублей. За повторное нарушение с 2015 года штраф составит от 10 до 20 тыс. рублей или дисквалификация на срок от одного года до трех лет (статья 5.27 КоАП РФ).

Дисциплинарная ответственность

Трудовой договор с работником может быть расторгнут по причине разглашения охраняемой законом тайны, ставшей известной в связи с исполнением трудовых обязанностей. В том числе и по причине разглашения персональных данных другого работника (подпункт «в» п. 6 ч. 1 ст. 81 ТК РФ).

Материальная ответственность

В случае незаконного распространения информации о персональных данных работнику организации может быть причинен моральный вред. Работник может потребовать его возмещения от работодателя. Если вред был причинен по вине лица, ответственного за неразглашение данных, то работодатель впоследствии может привлечь виновного к материальной ответственности за нанесенный ущерб.

Гражданско-правовая ответственность

Если в результате нарушения норм, регулирующих хранение, обработку и использование персональных данных работнику причинен имущественный ущерб или моральный вред, то он подлежит возмещению в денежной форме в соответствии гражданским законодательством (статья 151 ГК РФ).

Уголовная ответственность

Если работник, ответственный за хранение, обработку и использование персональных данных злоупотреблял своими служебными полномочиями, распространял сведения о частной жизни других работников без их согласия, то он может быть привлечен к уголовной ответственности на основании статьи 137 УК РФ.

Проверки

Как уже говорилось выше, ведомством, которое уполномочено контролировать соблюдение режима персональных данных, является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. Однако права налагать и взыскивать штрафы у этой организации нет. Все материалы по тем проверкам, где обнаружены нарушения, Роскомнадзор передает в прокуратуру. Прокурор уполномочен принимать решения о возбуждении производства по административному правонарушению (п. 1 ст. 28.4 КоАП РФ). Вопрос же о наложении штрафов решается судьей (п. 1 ст. 23.1 КоАП РФ).

Положение о персональных данных

Теперь попробуем выяснить, что же требуется сделать, чтобы успешно пройти проверку Роскомнадзора и избежать штрафов.

Вопросы обработки персональных данных регулируются Федеральным законом от 27.07.06 № 152-ФЗ «О персональных данных» (далее — Закон № 152-ФЗ). Соблюдать требования этого закона должны все организации и ИП, у которых есть хотя бы один работник.

Главным документом, который должен иметь любой работодатель, является положение о персональных данных. Принять этот локальный акт, регулирующий порядок хранения и использования персональных данных работодателя обязывает статья 87 Трудового кодекса. В положении обычно прописывают все

требования к получению, хранению, комбинированию, передаче и любому другому использованию персональных данных, а также гарантии по их защите.

На практике такой документ обычно состоит из разделов, описывающих каким именно образом в организации должен происходить сбор и обработка персональных данных; кто и в каком порядке имеет доступ к этим данным; какие меры предпринимаются для предотвращения разглашения персональных данных.

Так что начать Положение мы рекомендуем с раздела «Сбор и обработка персональных данных». В нем обязательно нужно зафиксировать, что персональные данные в организации можно получить и обрабатывать исключительно на основании письменного согласия работника. А значит, не лишним будет сразу разработать и утвердить форму такого заявления. На подпись такое заявление работнику надо давать сразу при приеме на работу. А по действующим сотрудникам такую работу придется провести сразу же после утверждения Положения.

Далее может следовать раздел «Доступ к персональным данным». В нем последовательно описывается порядок доступа к таким данным работников организации и третьих лиц. При необходимости тут можно ввести уровни доступа в зависимости от должности сотрудника. Например, директор и аппарат дирекции имеют доступ ко всем персональным данным; сотрудники бухгалтерии — только к тем сведениям, которые необходимым для расчета заработной платы и налогов; представители кадровой службы — к сведениям, необходимым для оформления кадровой документации и т п.

Продолжит Положение раздел «Порядок обработки и передачи данных». Здесь надо зафиксировать правила для передачи данных о сотрудниках определенным органам или лицам. В случаях, когда передача данных регулируется законодательно (налоговые органы, органы статистики, Пенсионный фонд и т п.) достаточно сделать ссылки на порядок передачи сведений, установленный законодательством. Но при этом следует обязательно зафиксировать, кто и в каком порядке вправе готовить данные сведения для передачи в госорганы.

<<...Главным документом, который должен иметь любой работодатель, является положение о персональных данных...>>

А вот родственникам, членам семьи, страховым компаниям, банкам, благотворительным организациям, негосударственным пенсионным фондам и т п. персональные данные предоставляются только при наличии письменного согласия работника на каждый конкретный факт передачи данных.

Закончить Положение лучше разделом «Ответственность». Тут изобретать велосипед не нужно — достаточно будет сделать ссылки (или привести целиком) на нормы Трудового кодекса (увольнение за разглашение персональных данных по статье 81 ТК РФ), Кодекса об административных правонарушениях (уже знакомая нам статья 13.11 КоАП РФ) и, если есть такая необходимость Уголовного кодекса (ст. 137 УК РФ).

Положение о персональных данных можно разработать, взяв за основу разработанный нашим юристом образец «Положение о работе с персональными данными».

Однако кроме положения контролирующие органы в ходе проверок интересуются и другими документами. Назовем некоторые из них.

Приказ руководителя о назначении ответственного

Руководитель должен издать приказ о назначении ответственного за работу с персональными данными и обеспечении их защиты. Таким ответственным может быть как конкретное лицо (см. образец «О назначении ответственного за работу с персональными данными и обеспечение их защиты (ответственное лицо)»), так и подразделение. В последнем случае личную ответственность несет руководитель такого подразделения.

Перечень персональных данных

Также потребуется утвердить документ, содержащий перечень персональных данных (см. образец «Приказ об утверждении перечня персональных данных»), которые реально используются в деятельности организации. Составляя такой документ, не забудьте включить в него все сведения, которые работник письменно сообщает о себе при поступлении на работу, а также используемые в дальнейшем при оформлении кадровой документации.

В этом перечне должны быть: заявление о приеме на работу; анкета сотрудника; личная карточка; личное дело; трудовой договор; приказы; трудовая книжка; материалы аттестационных комиссий.

Это один раздел перечня. Если же в организации имеется внутренний документооборот, содержащий сведения о сотрудниках (например, отчеты и материалы, которые составляются для акционеров, учредителей, головной организации и т п.), то эти отчеты тоже нужно включить в перечень.

Помимо этого, в перечне должны быть указаны документы, содержащие те сведения о сотрудниках, которые организация представляет в различные государственные органы (налоговую и трудовую инспекции, органы статистики).

Журнал учета персональных данных

Работодатели обязаны соблюдать режим конфиденциальности персональных данных (статья 7 Закона № 152-ФЗ). В подтверждение того, что названное требование соблюдается, контролирующие органы могут потребовать представить журнал учета персональных данных, где указано, кто и когда имел доступ к

конфиденциальной информации. Заметим, что форма такого журнала не установлена, поэтому разработать ее требуется самостоятельно.

Внешняя и внутренняя защита персональных данных

Угрозы для хранящихся персональных данных, условно, можно разделить на внешние и внутренние.

Если говорить о защите от внешних угроз, то в локальных актах имеет смысл прописать особый режим доступа в помещения, где хранится информация, содержащая персональные данные. В частности, можно предусмотреть пропускной режим и контроль за посетителями офиса.

Что же касается внутренней защиты, то целесообразно регламентировать состав работников, обязанности которых требуют доступа к персональным данным. Конкретный перечень работников и случаи получения информации следует утвердить приказом или распоряжением (в котором оговорить, что, например, юристы компании могут получать персональные данные для оформления доверенностей).

Возможное решение

Очевидно, что решение вопросов, касающихся персональных данных, может отнимать у бухгалтера очень много времени: требуется изучить весьма объемный закон и понять, какие действия надо совершить, какие документы составить, найти примерные образцы этих документов, скорректировать и заполнить их.

Если учесть, что общее количество документов и действий по обработке данных исчисляется десятками, можно представить, сколько времени и сил потребуется бухгалтеру, чтобы организовать работу с персональными данными в соответствии с требованиями закона.

Сэкономить время и сосредоточиться на своей основной работе можно с помощью веб-сервиса «Персональные данные». Он автоматически формирует все необходимые приказы, акты, уведомления и положения, необходимые для работы с персональными данными. Вопросы, возникающие в ходе совершения действий, бухгалтер прямо со страницы сервиса может задать эксперту и получить оперативный ответ. Когда все действия завершены, остается только распечатать подготовленные сервисом документы и подписать их. Впоследствии сервис будет напоминать, что пора провести определённое мероприятие, закреплённое в комплекте документов, а также следить за изменениями законодательства и информировать о том, что надо сделать после вступления поправок в силу.

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».

Только 4 из 10 пользователей интернета в России заботятся о безопасности своих почтовых паролей

15 сентября 2014, Россия, Москва
Источник: sia.ru

Лишь немногие российские пользователи интернета хоть что-нибудь предпринимают для того, чтобы защитить свои персональные данные, выяснил Исследовательский центр портала Superjob. По данным опроса 1600 экономически активных россиян, 49% из них ничего не делают для защиты своей приватной информации во Всемирной сети. Озаботились проблемами компьютерной безопасности 16% респондентов. Больше трети (35%) затруднились дать ответ.

Мужчины вдвое чаще женщин стараются защитить свои данные от непрошеных гостей (22% и 11% соответственно). Наиболее осторожны россияне в возрасте от 35 до 44 лет: стремятся обезопасить свою личную информацию 19% таких респондентов. А вот хорошо разбирающаяся в интернет-технологиях молодежь относится к безопасности к сети без особого трепета: в группе опрошенных до 24 лет только 11% активно защищающих свои интернет-данные, но при этом 42% затруднившихся ответить.

Большая доля затруднившихся с ответом (как среди молодежи, так и в целом) косвенно свидетельствует, что среди населения отсутствуют четкие представления о том, как защитить персональные данные в Сети.

Что в представлении россиян защита данных в Интернете? 28% тех, кто считает нужным это делать, устанавливает на свою почту или личные страницы сложные пароли, каждый пятый (20%) полагается на антивирусные программы, 19% часто меняет пароли. По 11% взяли за правило предоставлять о себе в открытом доступе минимум информации или вообще не размещать в Сети персональных данных. 6% россиян ограничивает доступ к личным данным или персональной странице в интернете, каждый двадцатый принципиально не регистрируется в соцсетях. 3% избегают заходить на подозрительные сайты, по 2% устанавливают двойное подтверждение входа в интернет, изобретают собственную систему шифрования или определяют особые настройки приватности. 17% назвали другие способы, позволяющие защитить себя в интернете. Например, подключают к счету систему смс-информирования, намеренно искажают личные данные, регистрируясь на сайтах, пользуются советами знакомых программистов и т.д.

Те же, кто мало озабочен проблемами безопасности своих личных данных, как правило, говорили, что им нечего скрывать или признавались, что просто не знают надежных способов защиты от компьютерного взлома. «Кому я нужен?» — утверждение частое, но малоубедительное.

<<...Не особенно серьезно относятся российские интернет-пользователи к выбору почтовых паролей...>>

Не особенно серьезно относятся российские интернет-пользователи к выбору почтовых паролей. 50% граждан отдают предпочтение удобным, а не безопасным паролям. 40% подходят к делу основательно и «шифруются» на совесть, каждый десятый ответа не дал.

Мужчины снова оказались предусмотрительнее женщин: сложным паролям отдают предпочтение 45% и 36% соответственно. Более изобретательны молодые пользователи – 51% тщательно продумывают заветную комбинацию цифр и букв, выбирают простые сочетания 38%. Старшее поколение действует диаметрально противоположным образом: 31% респондентов в возрасте за 45 лет придумывает сложные пароли, 59% — пользуется теми, что попроще. Люди с невысоким доходом гораздо более бдительны, чем обеспеченные россияне. Понимают, что простота ведет к воровству, и выбирают сложные коды доступа 44% граждан с доходом до 25 тысяч рублей в месяц и всего 38% самых обеспеченных респондентов.

Изобретатели нестандартных сложных паролей подходят к делу творчески. Они пользуются мнемонической техникой или выбирают в качестве ключевых слов фразу из произведения никому не известного автора.

При этом некоторые респонденты объясняли, что сложные пароли им ни к чему. «Не передаю по электронной почте важную информацию»; «Взломать любой пароль сегодня не проблема, как раньше открыть дверцу почтового ящика»; «Главное — это выбрать такой пароль, чтобы самой потом его не забыть», — говорили они.

Но сейчас, после скандала вокруг появления в доступе сразу нескольких баз данных о паролях адресатов электронной почты на популярных бесплатных серверах, возможно, кто-то пересмотрит свое отно-

шение к проблеме безопасности в Сети. «Подумываю о более сложном пароле»; «Я начинающий пользователь и выбираю более красивый пароль. Возможно, в будущем отнесусь более серьезно», — пояснили респонденты.

Лаборатория Касперского и компания B2B International провели исследование о последствиях детских шалостей в Интернете

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

То, что дети часто пользуются электронными гаджетами своих родителей, уже давно никого не удивляет. Но в последнее время, вместе с развитием мобильных устройств и электронной коммерции, детские игры рискуют поставить под угрозу данные родителей и их кошельки. Корпорации Google и Apple уже привыкли оплачивать родителям сетевые шалости их отпрысков.

Как сообщается в исследовании, проведенном Лабораторией Касперского и исследовательской компанией B2B International, дети 12% пользователей, пользуясь их компьютерами, случайно удаляли важную информацию. А 14% респондентов отметили, что, разрешая детям пользоваться своими гаджетами, теряли важную информацию или денежные средства.

Оплата за виртуальные покупки в магазинах приложений списывалась с банковских счетов у 2% пользователей. Эти действия, а также покупки внутри приложений — одна из главных финансовых опасностей использования детьми родительских мобильных устройств.

Такое количество пострадавших от детских развлечений в интернете вполне закономерно, учитывая, что 45% опрошенных аналитиками родителей считают, что их дети не знают ничего о компьютерной безопасности, а 43% уверены, что их дети недостаточно хорошо разбираются в технологиях.

Несмотря на то что встроенные в приложения покупки, как правило, не слишком дороги, они могут принести родителям серьезный финансовый ущерб: так, две недели назад корпорация Google обязалась компенсировать пострадавшим от детских покупок пользователям не менее $19 млн. Ранее в этом году возместить по меньшей мере $32,5 млн согласилась и Apple.

Методы, используемые россиянами для защиты своих данных от детей, а детей — от интернет-угроз в основном достаточно базовые: 36% опрошенных родителей ограничивают время, которое дети проводят в интернете, а 24% просматривают историю браузера. Столько же родителей заявили, что регулярно проводят с детьми беседы о необходимости соблюдения интернет-безопасности.

При этом всего 19% родителей используют специальное ПО, так называемый родительский контроль — программы, позволяющие ограничивать доступ с детских устройств к сайтам по различным критериям, запретить запуск определенных программ или ограничить время работы компьютера. Однако именно этот метод рекомендуют эксперты по интернет-безопасности.

Использование родительского контроля не — проявление недоверия к ребенку, а разумная мера предосторожности, позволяющая в том числе защитить устройство и данные на нем, говорит руководитель группы анализа веб-контента Лаборатории Касперского Константин Игнатьев.

Впрочем, этот же инструмент может применяться и взрослыми детьми для защиты от киберугроз своих родителей, отмечает Игнатьев.

КОМПЕТЕНТНОЕ МНЕНИЕ:
Алексей Оськин, ESET Russia, руководитель отдела технического и маркетингового сопровождения

<<Наиболее эффективный способ защиты счета для родителей – отказ от привязки банковских карт к аккаунтам на веб-сайтах или в мобильных приложениях. Как вариант, создавайте для детей персональные аккаунты без доступа к родительским финансам. При этом убедитесь, что ребенок не сможет войти в вашу учетную запись с помощью автоматического ввода логина и пароля.
Если родители пользуются с ребенком одним и тем же компьютером, планшетом или смартфоном, им следует регулярно проверять устройство на предмет сохранности своих персональных данных.>>

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.

<<...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...>>

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.>>

Леонид Левин рассказал об основах информационной безопасности

30 сентября 2014, Россия, Москва
Источник: riasv.ru

Леонид Левин, председатель думского комитета по информационной политике

Избранный в конце сентября председателем думского комитета по информационной политике, информационным технологиям и связи Леонид Левин рассказал «Известиям» о планах нижней палаты парламента в области обеспечения информационной безопасности страны.

Вопрос: Как председатель комитета по информационной политике вы будете формировать основную повестку. Что в нее войдет?

Леонид Левин: Сегодня законотворческая экспертная работа комитета должна быть направлена на формирование основ общегосударственной информационной политики на много лет вперед. Мы должны сохранить и расширить наши достижения в информтехнологиях, защитить наше государство и общество в условиях новых информационных вызовов и обеспечить разумный баланс комфорта и безопасности пользователям интернета и сетей связи.

Вопрос: В свете ведущейся информационной войны стоит ли ожидать новых законодательных инициатив? Может быть, следует ждать ужесточения законодательства?

Леонид Левин: Мы живем в достаточно сложном информационном пространстве. Разоблачение Сноудена, последующее обострение международной обстановки, кибератаки на органы госвласти на всех уровнях, утечки личных данных огромных масштабов, небывалых ранее, — всё это выводит тему киберпространства и технологий связи на первый план. Еще одна проблема — это демонизация нашей страны в мировых СМИ, запрет трансляции российских каналов. Это делает тему информационной политики безусловно приоритетной. Поэтому бурное развитие информационных технологий, которое за последние десятилетия изменило информационную картину мира, поставило перед комитетом новые вопросы, которые предстоит решать. Это вопросы правового регулирования интернет-пространства, защиты персональных данных граждан и компаний, защиты государственных секретов и национальной безопасности. А также недопущения использования новых каналов связи в криминальных и террористических целях. Вот ключевые аспекты, над которыми нам нужно работать. В последнее время Государственной думой принят ряд новых законов и поправок в действующие законодательные акты. Мы обязаны и дальше мониторить ситуацию и своевременно отвечать на новые вызовы времени и запросы общества.

Вопрос: Перед вашим комитетом стоит очень сложная задача — информационная безопасность. Если государство сможет защитить свои ресурсы, то простых людей защитить тяжело в Интернете. Что будете предпринимать в этом направлении?

Леонид Левин: Законодательство должно основываться на защите персональных интересов граждан. Решение, который было принято в мае Высшим судом справедливости Евросоюза, позволяет требовать удаления из Сети ложной или не соответствующей действительности информации. Это как раз то, что необходимо России. Это именно тот случай, когда нам стоит брать пример с Европы.

Там на сегодняшний день эта ситуация упростилась. Даже появились интернет-роботы, которые предлагают за небольшую плату заполнить анкету по обращению на порочащую информацию, и отслеживают его реализацию у интернет-компании. Если поисковик признает, что она соответствует определенным прописанным нормам, то она должна быть удалена.

Вопрос: По линии различных организаций, к примеру таких как ОДКБ, принимается много документов, касающихся информационной безопасности…

Леонид Левин: Сейчас будет очень много работы. Информация управляет миром. Но сегодня не время новостей, а время интерпретаций. На саму новость уже никто не смотрит, всем интересно, как ее интерпретируют. И здесь очень важно, чтобы мы не давали возможность создавать условия, при которых будет допустимо искажать новостные события. Нужно стараться, чтобы информация максимально объективно доходила до читателя и зрителя. К тому же необходимо доносить нашу позицию не только до российских, но и до иностранных СМИ.

Вопрос: Первый законопроект после ухода Митрофанова, который выйдет уже под вашей эгидой, — об ограничении доли иностранцев в СМИ. Скоро он вступит в силу, но многие всё равно выступают против него. Звучат предложения применять его только к общественно-политическим изданиям, а различные развлекательные СМИ не трогать. Ваше отношение к таким предложениям?

<<...Информация управляет миром. Но сегодня не время новостей, а время интерпретаций. На саму новость уже никто не смотрит, всем интересно, как ее интерпретируют...>>

Леонид Левин: Этот закон не об информационной политике, а об имущественных отношениях. Сейчас, когда на наше государство оказывается прямое давление в виде санкций, когда в его адрес высказываются прямые угрозы респектабельными зарубежными государственными деятелями, мы используем зарубежный законодательный опыт и упорядочиваем ситуацию в информационной сфере. Мы не можем допустить, чтобы в этой связи каким-то образом происходило административное воздействие через иностранных собственников на наше отечественное и зарубежное медиапространство.

Вопрос: А как в дальнейшем будут строиться взаимоотношения государства с филиалами иностранных СМИ — например, с Euronews или с BBC? Их же тоже нужно переводить в российскую юрисдикцию?

Леонид Левин: Я думаю, что этот вопрос потребует дальнейшей детализации и проработки, в случае если такая необходимость возникнет. Но мы считаем, что западные компании, особенно имеющие у нас свои представительства, смогут найти форму «сохранения и продолжения» работы на территории РФ. Мы не собираемся изолировать страну от взаимодействия с миром. И особенно зарубежные журналисты, освещающие события в нашей стране, безусловно, должны продолжать полноценно работать на территории России.

Вопрос: Хотелось бы подробнее узнать про эту 25-процентную долю. Выходили ли на вас издатели глянцевых изданий? Они заявляли, что могут подать в суд, оспорить это решение. Есть такая вероятность?

Леонид Левин: В силу происходящих событий закон принимался достаточно быстро, поэтому, возможно, у кого-то остались вопросы. Мы понимаем, что все довольными быть не могут, особенно когда в закон включены определенные ограничения. Но многие страны с успешными экономиками и развитыми медиа имеют такие же законы, а в некоторых странах даже более жесткие. При ограничении доли мы не ограничиваем право собственности и право на дивиденды — они полностью сохраняются.

Очень важным аспектом закона является деофшоризация в области СМИ, потому что очень многие из них фактически российские, но зарегистрированы за границей. И следствием осуществления этого закона будет дальнейшая деофшоризация экономики РФ и улучшение прозрачности прав бизнеса, увеличение налоговой базы от медиаотрасли.

Вопрос: С 1 января следующего года сервер с персональными данными россиян они должны будут хранить исключительно на территории страны. Чисто технически это возможно будет сделать? Как происходит взаимодействие в этом плане с персональными данными в Facebook и других соцсетях?

Леонид Левин: Мы не можем допустить, чтобы вследствие межгосударственной напряженности страдала личная жизнь наших граждан, мы должны защитить их личные данные. В этой связи данный закон и принят. Именно для того чтобы люди, которые регистрируются на различных сайтах, знали и понимали, что их данные хранятся на территории РФ и не могут быть использованы в противоправных целях. Представляя данный законопроект, я уже говорил, что часто различные государственные и муниципальные органы, коммерческие организации, обрабатывающие персональные данные, хранят их на серверах за границей без ведома граждан.

С другой стороны, мы должны думать и о том, что санкции в отношении России могут расширяться и касаться в том числе и информационных технологий. И в этой связи мы должны сделать всё, чтобы использование информационных технологий против нашей страны не привело к отключению серверов и коллапсу отечественных информационных систем. Очень важно, чтобы люди независимо от межгосу-

дарственных отношений и проблем продолжали пользоваться и обмениваться информацией между собой.

Вопрос: Но диалог с такими гигантами, как Facebook, ведется?

Леонид Левин: Его ведет в первую очередь Роскомнадзор. Мы находимся с ним в контакте, и они нас информируют о том, как идет этот диалог. Мы считаем, что Россия с точки зрения аудитории приносит таким компаниям большой доход. Это не только Facebook и Twitter, но и такие многопрофильные гиганты, как Google. Я думаю, что все они крайне заинтересованы в том, чтобы продолжать работу на территории РФ. С ними продолжается диалог не о том, будут они следовать закону или нет, а о том, как создать предпосылки, чтобы они принимаемое законодательство выполняли в срок.

Вопрос: А что касается защиты самих чиновников и других важных лиц от вскрытия хакерами их лично переписки? Говорилось о том, что они должны всю служебную информацию хранить на своих служебных почтовых ящиках.

Леонид Левин: Сейчас обсуждается много различных законопроектов, связанных с информационными угрозами и внешними вызовами. Ведь Россия жила долгое время в условиях полностью нерегулированного интернета и крайне свободного информационного пространства. Эта ситуация приучила всех нас, что и интернет и другие средства связи — эта зона беззакония. Но интернет — эта такая же среда для человека, как воздух и вода, и она должна быть приведена в правовое поле.

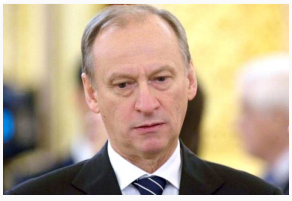
Свобода каждого заканчивается, когда начинается свобода другого. Поэтому как беззаконие нетерпимо на улице, так оно должно быть нетерпимо и в интернете. Конечно, приходится принимать и неприятны для отдельных лиц и компаний решения, но это неизбежно, если мы хотим обеспечит безопасность и устойчивое развитие нашего общества в целом. Возвращаясь к вашему вопросу, мы должны принять все меры, чтобы быть готовым к сегодняшним информационным вызовам.

Вопрос: Ваши коллеги по Госдуме предлагали создать что-то вроде киберполиции, чтобы отслеживали нарушения в отношении пользователей...

Леонид Левин: У нас право на личную переписку и частную жизнь никто не отменял. Интернет в нашей жизни играет важную роль, поэтому начиная от личного достоинства, безопасности наших близких до авторского права, всё должно быть защищено. А это огромный труд, который требует концентрации и внимания ежедневно. С учетом влияния и развития интернета роль Роскомнадзора будет усиливаться — он должен получать новые полномочия и расширять зону действия. Но есть и общественные организации, которые часто подключаются к этой проблеме. И такая общественная поддержка со стороны пользователей — это очень важно.

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.

Бизнес спросил кремлевских юристов про закон о персональных данных

02 октября 2014, Россия, Москва
Источник: top.rbc.ru

Компании не понимают, как работать с новым законом о персональных данных, уведомила правовое управление президента Ассоциация европейского бизнеса (АЕБ). Закон требует, чтобы личные данные россиян хранились в России с 1 сентября 2016 года, и, возможно, дата будет приближена. Кремлевские юристы не успокоили предпринимателей: по их мнению, закон распространяется на все виды бизнеса, а также на информацию, переданную до его принятия. Кроме того, нельзя иметь копии данных за рубежом

Никаких исключений

Государственно-правовое управление президента России ответило на запрос генерального директора Ассоциации европейского бизнеса Франка Шауффа 18 сентября (копия есть у РБК). Эта ассоциация была создана в 1995 году и включает сегодня более 650 компаний разных отраслей, в числе которых такие крупные бренды, как Bayer, Deloitte, Home Credit and Finance Bank.

Юристы отметили, что к «компетенции управления не относится разъяснение норм законодательства РФ», но согласились «высказать отдельное мнение».

Глава АЕБ спрашивал, не будет ли противоречить закону обработка персональных данных за рубежом, если хранить в России «дублирующие базы», а также получать согласие самих россиян на это. Кроме того, европейцы надеялись на исключение из закона – если оператор данных работает на основании международных договоров.

Управление не стало обнадеживать бизнесменов: в ответе помощника президента и начальника управления Ларисы Брычевой подчеркивается, что в законе «отсутствует упоминание о дублирующих базах данных или актуальных копиях данных».

«Если на оператора возложены функции, полномочия и обязанности, выполнение которых связано с достижением целей, предусмотренных международным договором или законом», новые правила хранения данных не будут применяться, согласились юристы. Но на просьбу АЕБ предоставить список таких договоров управление ответило отказом. В письме приведены примеры: хранить данные за рубежом можно, если это необходимо «для правосудия и исполнения решений исполнительной власти», «для оказания государственных и муниципальных услуг», «для работы СМИ, научной, литературной и иной творческой деятельности».

<<...С персональными данными работают сайты многих компаний: социальные сети, почтовые службы, сервисы по продаже авиабилетов и др...>>

Под действие закона подпадают все операторы, категоричны юристы: «Закон не содержит каких-либо изъятий относительно отдельных видов операторов».

Ассоциацию также волновало, распространяется ли вступающий в силу в 2016 году закон на уже переданные данные. Управление заключило, что «запреты, установленные законом, распространяются и на те персональные данные, которые были ранее переданы за пределы России».

Источники, близкие к Ассоциации европейского бизнеса и отраслевой российской ассоциации, подтвердили подлинность письма. От официальных комментариев в АЕБ отказались. Управление президента России не ответило на запрос РБК.

Хранить персональные данные россиян в России требует принятый в июле закон №242 «О внесении изменений в отдельные законодательные акты РФ в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» (известен как закон о персональных данных). Он устанавливает срок переноса серверов с данными на сентябрь 2016 года. Но депутаты хотят перене-

сти вступление закона в силу на 1 января 2015 года. Такую поправку уже приняли во втором чтении в Госдуме в конце сентября.

С персональными данными работают сайты многих компаний: социальные сети, почтовые службы, сервисы по продаже авиабилетов и др. Различий по категориям данных в законе нет: «Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)», – сказано в документе.

Нарушителей будут заносить в специальный реестр, а если сайт, на котором было обнаружено нарушение, не отреагирует на предписание Роскомнадзора, его ждет блокировка. Один из авторов закона, депутат Госдумы от ЛДПР Вадим Деньгин затруднился ответить РБК, как будут проходить проверки, – этот вопрос, по его мнению, должны проработать технические специалисты, а он сам технически не подкован. Деньгин заверил, что с отраслью этот вопрос обсуждается.

Директор по стратегическим проектам Института исследований интернета Ирина Левова считает, что ответ управления однозначен: все данные должны храниться исключительно на территории России. На том, что копии за рубежом недопустимы, настаивает и Деньгин. «Зарубежные компании могут втихую хранить данные, но это будет нарушать закон», – считает депутат.

КОМПЕТЕНТНОЕ МНЕНИЕ:

Карен Казарян, Российская ассоциация электронных коммуникаций , ведущий аналитик

<<Может признаваться приоритет международных договоров, а значит, и 108-й конвенции Совета Европы. Трансграничная передача, таким образом, не запрещается, равно как и все технические меры, необходимые для нее, то есть дублирующие базы. Международных соглашений в разных сферах множество, например у авиакомпаний есть мнение, что на продажу билетов новая норма не распространяется, потому что ее покрывают другие межправительственные соглашения об авиаперевозках.>>

Лариса Третьякова: Рунет нуждается в саморазвитии

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

Лариса Третьякова, доверенное лицо Президента РФ

Доверенное лицо Президента РФ комментирует выступление главы государства на заседании Совбеза 1 октября:

- Сегодня во всем мире вопросам информационной безопасности уделяется повышенное внимание. Базы данных, массивы информации, персональные данные – тот же клад, которым, если он плохо лежит, стремятся воспользоваться мошенники.

СМИ сообщают нам о хакерских атаках на сайты, взломах систем защиты и воровстве в Интернете, списании денег с чужих банковских счетов и так далее. С помощью интернет - технологий прекрасно режиссируются протестные спектакли, нагнетается негатив, действуют международные террористические организации, религиозные секты.

У государственных органов, работающих с персональными данными граждан – свои мотивы защиты информации. В первую очередь, это необходимо для исполнения действующего законодательства. Президент абсолютно ясно дал понять, что тем самым власть защищает граждан от рисков, связанных с утечкой и незаконным использованием прежде всего их персональных данных. Также глава государства подчеркнул, что ограничения по доступу в интернет, пользованию теми или иными законно существующими ресурсами, никто не вводит.

Российский сегмент Сети нуждается в саморазвитии, нужны собственные технологии и программы. Наличие отечественного общедоступного программного ресурса будет означать лишь одно: Россия станет сильнее.

Летом Правительство РФ внесло существенные изменения в ряд нормативных актов по вопросам использования интернета

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

Постановление Правительства от 31.07.2014 № 758 привело не только к очередному скандалу в интернет-среде, но и прибавило хлопот отечественным организациям. Так, в их адрес от провайдеров в стали приходить письма с неоднозначными требованиями, явно противоречащими закону.

В своих письмах провайдеры требуют от абонентов - организаций и предпринимателей предоставления списка работников, пользующихся интернетом на своем рабочем месте. Причем с указанием фамилии, имени, отчества, места жительства, а также данных паспорта. Данный список должен быть заверен уполномоченным представителем юридического лица либо индивидуальным предпринимателем, и обновляться не реже одного раза в квартал.

С предложением обсудить на сайте подобные требования операторов связи в редакцию Клерк.Ру обратилась сотрудница компании, в чей адрес как раз и было направлено похожее письмо. В письме содержалась просьба провайдера подписать дополнительное соглашение к договору на предоставление услуг связи и раскрыть персональные данные всех сотрудников компании, пользующихся данными услугами. Подписать допсоглашение руководство предприятия отказалось, сославшись на то, что обязанность в предоставлении оператору связи юридическим лицом списка лиц, использующих его пользовательское оборудование, противоречит ФЗ от 27.07.2006 г №152-ФЗ «О персональных данных».

Отказ компании был мотивирован следующим. В силу данного закона (статья 5) обработка персональных данных должна осуществляться на законной и справедливой основе. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Кроме того, обработка персональных данных осуществляется с согласия субъекта персональных данных.

Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, а в поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке. В свою очередь лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

<< *...В своих письмах провайдеры требуют от абонентов - организаций и предпринимателей предоставления списка работников, пользующихся интернетом на своем рабочем месте...* >>

"Таким образом, Вы не одно из вышеперечисленных норм закона не выполнили и данные запрашиваемые Вами не могут быть предоставлены", - заключает руководство компании в ответе на письмо провайдера.

Представляется, что все подобные требования не соответствуют нормам законодательства и могут просто игнорироваться работодателями. Без каких бы то ни было последствий (никаких санкций за это не предусмотрено).

Действительно, по новым правилам в договоре с абонентом - юридическим лицом либо индивидуальным предпринимателем, предусматривается обязанность предоставления оператору связи списка лиц, использующих его пользовательское (оконечное) оборудование, и устанавливается срок предоставления указанного списка, а также устанавливается, что указанный список должен содержать сведения о лицах, использующих его пользовательское (оконечное) оборудование. В частности, об этом гласит Постановление Правительства РФ от 23.01.2006г №32 «Об утверждении правил оказания услуг связи по передаче данных» (пункта 26.1) и Постановление Правительства РФ от 10.09.2007г №575 «Об утверждении правил оказания телематических услуг связи» (пункт 22.2).

Между тем, если допустить, что данные нормы касаются именно работодателей, придется признать, что внесенные изменения противоречат действующему федеральному законодательству, которое подобной обязанности не содержит. Более того, Трудовой кодекс РФ прямо запрещает разглашать персональные сведения сотрудников организаций.

В статье 88 кодекса указывается, что работодатель не должен не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных федеральными законами (постановления правительства, как известно, не являются федеральными законами).

Также работодатель должен осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным

актом, с которым работник должен быть ознакомлен под роспись, и разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций. Поэтому, на наш взгляд, нововведения затрагивают несколько иных субъектов, а не всех работодателей поголовно.

Как на самом деле

Во-первых, здесь необходимо понимать, для чего именно были внесены поправки в правила предоставления услуг связи. Во-вторых, следует различать случаи, на которые данные изменения распространяют свою силу, и те, на которые нет. Начнем сначала. Изменения были внесены с целью борьбы с преступлениями, совершаемыми с использованием интернета (те же самые заведомо ложные сообщения о терроризме), и повышения эффективности расследования данных преступлений. В указанных целях законодатель и определил перечень субъектов, обязанных предоставлять операторам связи данные о конечных пользователях.

Наверное, многие помнят шумиху, поднятую прессой и общественностью по поводу недавних странных публикаций с общим заголовком "Выход в интернет через Wi-Fi теперь будет строго по паспортам". Так вот это именно тот самый случай. Собственно, именно с целью установления контроля над пользователями интернета по Wi-Fi и были приняты нововведения. Как известно, проверить в случае необходимости работодателей не представляет особого труда. Даже если в компании работает несколько сотен сотрудников. Другое дело – проверить аэропорт, парк, кинотеатр и прочие места массового скопления пользователей интернета. Не имея данных о пользователях, раскрыть преступление в данном случае не представляется возможным.

Итак, кто же станет отчитываться перед провайдерами за пользователей интернета. В принципе уже сам закон "О связи" приводит перечень таких коллективных пунктов доступа. Так, по закону в каждом поселении должно быть установлено не менее чем одно средство коллективного доступа для оказания услуг телефонной связи с обеспечением бесплатного доступа к экстренным оперативным службам.

В поселениях с населением не менее чем пятьсот человек должно быть установлено не менее чем одно средство коллективного доступа для оказания услуг по передаче данных и предоставлению доступа к информационно-телекоммуникационной сети "Интернет" без использования пользовательского оборудования абонента. В населенных пунктах с населением от двухсот пятидесяти до пятисот человек, в которых установлено средство коллективного доступа для оказания услуг телефонной связи, должна быть установлена не менее чем одна точка доступа.

Львиная доля пунктов коллективного доступа приходится на отделения Почты России – в настоящее время их насчитывается порядка 21 тысячи по всей стране. Это что касается универсальных услуг связи. Между тем, изменения в подзаконные акты не исчерпываются универсальными услугами и охватывают еще и телематические услуги связи. Поэтому в список обязанных попадут (должны попасть) организации, где налажена раздача интернета по Wi-Fi.

Однако, новые правила отнюдь не означают, что в ближайшем будущем с посетителей кафе и ресторанов станут требовать предъявления паспортов и другой конфиденциальной информации. Скорее всего, для доступа в интернет потребуется лишь номер мобильного телефона – как известно, с недавнего времени сим-карты продаются исключительно по паспортам.

Поэтому проблем в данной части возникнуть по идее не может. Проблемы могут возникнуть именно с предоставлением бесплатного интернета в местах общего пользования. Сама по себе связь по Wi-Fi стоит копейки. Но вот другое Постановление Правительства Российской Федерации - от 31 июля 2014 г. N 759 г. обязывает организации хранить данные о пользователях и их интернет-соединениях. Приобретение же оборудования, позволяющего осуществлять данное хранение может вылиться в копеечку, что заставит кафе и бары пересмотреть свои взгляды на бесплатный интернет для посетителей.

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".

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

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, HOB 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 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 рестора-

нах 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!"

У каждого пятого россиянина украли аккаунт в соцсетях

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

У каждого пятого россиянина украли аккаунт в социальных сетях, показали результаты исследования «Лаборатории Касперского» и компании B2B International. Об этом пишет «Газета.Ру».

Отмечается, что большинство опрошенных (85%) не осознает связанные с этим риски и не соблюдает правила безопасности в Сети. Выяснилось, что 26% россиян заходят в социальные сети через публичный Wi-Fi, еще 41% респондентов сохраняют на своих устройствах логины и пароли от почтовых ящиков и аккаунтов в соцсетях.

По мнению 20% участников опроса, они публикуют о себе слишком много информации. Специалисты «Лаборатории Касперского» предостерегают пользователей от легкомысленного отношения к защите персональных данных. Кража информации может повлечь за собой неприятные последствия. Например, рассылку вредоносных файлов по списку контактов.

Зарубежная практика

Большинство латвийских компаний используют несложные пароли в интернет-банке

09 сентября 2014, Латвия
Источник: baltic-course.com

Две трети или 67% латвийских предприятий для входа в интернет-банк используют простые или средней сложности пароли, свидетельствует новейшее исследование банка Citadele Index, проведенное банком Citadele и центром исследования рынка и общественного мнения SKDS.

23% опрошенных предприятий ответили, что для работы с интернет-банком используют очень сложный пароль, например, содержащий не менее 10 символов и состоящий из прописных и строчных букв, цифр и специальных символов. В свою очередь, 10% опрошенных не смогли ответить на этот вопрос, сообщает БК Байба Абелниеце, руководитель корпоративных коммуникаций в банке Citadele.

Очень сложные пароли чаще используют средние и большие предприятия (соответственно, 39% и 37%). В свою очередь, среди микропредприятий для доступа в интернет-банк сложные пароли выбирает лишь каждый пятый.

Большая часть предприятий проблемы, связанные с безопасностью компьютеров и компьютерных сетей, решают своими силами — так ответили 64% опрошенных предприятий. В свою очередь, 22% компаний имеют договор с другим предприятием, отвечающим за компьютерную безопасность. Тем временем, почти каждое десятое или 9% предприятий на вопросы защиты компьютерных сетей не обращают внимания. 2% респондентов ответили, что на их предприятиях нет компьютеров, а 3% не смогли ответить на этот вопрос.

Так, треть представляемых респондентами предприятий являются также пользователями услуг SMS банка. 88% из них считают, что самым большим преимуществом SMS банка является возможность получать оперативную информацию о входящих перечислениях, 38% выше всего ценят оперативную информацию об исходящих перечислениях, 27% отметили возможность получать информацию о сделках с использованием платежных карт, в свою очередь, 15% считают, что это отличный способ контролировать доступный остаток на платежной карте.

Почти половина руководителей предприятий, использующих услугу SMS банка, обеспечивающую оперативное информирование на мобильный телефон о сделках по счету, считают, что данная услуга повышает уровень защищенности денежных средств клиента.

Перед началом работы с интернет-банком банк Citadele призывает обязательно проверить сертификат безопасности банковского сервера, который отображается в виде «ключика» в адресной строке интернет-банка. Кроме того, банк призывает своих клиентов быть осторожными, если при подключении к интернет-банку и вводе идентификационных данных образовалась длительная пауза и после этого повторно предлагается ввести пятизначный или шестизначный код, так как в этот момент, возможно, происходит попытка мошенничества. В таких случаях следует проверить компьютер с помощью антивирусной программы, а также сообщить об этом своему банку.

Организованный исследовательским центром SKDS опрос проводился в июне и в нем приняли участие 750 руководителей латвийских предприятий.

КОМПЕТЕНТНОЕ МНЕНИЕ:
Каспарс Цикмачс, Citadele, член правления

<<Для работы с интернет-банком рекомендуем не выбирать легко угадываемый пароль, например, такой, который ассоциируется с именем или персональными данными владельца компании. Чтобы пароль был надежным, он должен содержать от 8 до 20 символов, из которых хотя бы 6 символов отличаются друг от друга. Кроме того, в пароле обязательно должна присутствовать по крайней мере одна буква и одна цифра. По нашим наблюдениям, многие предприятия для обеспечения финансовой безопасности используют услугу SMS банка, информирующую о входящих перечислениях. Мы призываем предпринимателей подключить и другую функцию SMS банка, которая дает возможность контролировать исходящие операции, тем самым позволяя оперативно выявлять попытки мошенничества.
Заботясь о безопасности финансов своих клиентов, банк Citadele каждый год вкладывает несколько миллионов евро в развитие и обеспечение безопасности банковских систем. Однако с развитием информационных технологий и возможностей интернета, в мире, к сожалению, учащаются мошеннические попытки завладеть персональными данными людей, которые впоследствии используются в преступных схемах мошенников. Поэтому, чтобы безопасно пользоваться предоставляемыми современными информационными технологиями и интернетом возможностями, особенно важно, чтобы каждый из нас заботился о защите своих персональных и финансовых данных, и они не оказались в руках мошенников.>>

Google организует серию публичных встреч в европейских городах, чтобы обсудить право на хранение и удаление личных данных пользователей

10 сентября 2014, Евросоюз
Источник: feedage.com

Google планирует провести 7 публичных собраний в европейских столицах и вынести на обсуждение противоречие, возникающее в ходе реализации прав человека на свободу информации и на конфиденциальность личных данных, сообщает Computerworld. Консультативный Совет Google провел первое собрание 9 сентября в Мадриде. Затем общественные обсуждения состоятся в Риме, Париже, Варшаве, Берлине и Лондоне. Последняя встреча пройдет в Брюсселе 4 ноября.

"Европейский Суд вынес решение, в соответствии с которым каждый человек имеет право потребовать от поисковых систем убрать из поиска результаты, включающие его имя и персональные данные, – говорится в заявлении Консультативного Совета Google. – С тех пор, мы стали получать просьбы по удалению самого разнообразного контента: сведений о прошлых судимостях, неприличных фотографий, проявлений онлайн-агрессии, непопулярных мнений многолетней давности, негативных отзывов в прессе и пр."

Google внимательно изучает каждый такой запрос, взвешивая все аргументы пользователя, имеющего право на конфиденциальность данных, против права других граждан на свободный доступ к подобной информации.

"Мы хотим, чтобы эти два закона работали сбалансированно, – говорят в Google. – Это новое обязательство представляет для нас камень преткновения, и потому мы спрашиваем общественного мнения, что-

бы решить, каким образом Google должен принимать решения в подобной ситуации. Мы только начинаем разрабатывать свод соответствующих правил, и нам интересно ваше мнение. Этот закон касается непосредственно ваших онлайн-прав, а интернет предоставляет отличную возможность для дискуссий и дебатов."

Прошлой весной Европейский суд вынес решение, в соответствии с которым любой человек имеет право отредактировать свою персональную историю в поисковых системах Google. Это значит, что любой пользователь имеет право потребовать от поисковых систем, таких как Google, Yahoo или Bing, удалять ссылки на устаревшую информацию в поисковиках. Суд заключил, что любой человек имеет право на интернет-забвение.

Сегодня каждый человек имеет право подать запрос через сайт поисковой системы на удаление своих персональных данных и другой компрометирующей информации из поисковиков. Google изучает запрос и приходит к заключению, насколько релевантна данная информация. Если информация потеряла свою актуальность, все ссылки на содержащую ее страницу должны быть удалены.

Оценкой каждого подобного запроса занимается специально созданный Экспертный совет, в состав которого входит 10 человек, в том числе председатель совета директоров Эрик Шмидт (Eric Schmidt); Люсиано Флориди (Luciano Floridi), профессор философии и информационной этики Оксфордского Университета; Сильвия Кауфман (Sylvie Kauffmann), директор издательства французской газеты Le Monde; Лидия Колука-Цук (Lidia Kolucka-Zuk), генеральный директор Варшавского Фонда Гражданского Общества по Центральной и Восточной Европе.

Результаты работы Экспертного совета публикуются и призваны стать основой политики компании в области права человека на интернет-забвение.

"Совет также приглашает государственные органы, бизнес-объединения, медиа-ресурсы, академические учреждения, компании, работающие в сфере ИТ и защиты данных и в других смежных областях внести свой вклад в разработку политики разрешения подобных ситуаций, обсудить вопрос о том, как можно сбалансировать права общества на доступ к информации и право индивида на конфиденциальность личных данных," – отметили представители Google.

У американской прокуратуры возникли неудобные вопросы к Apple Watch

17 сентября 2014, США
Источник: i-ekb.ru

Умные часы Apple Watch породили массу вопросов, связанных с приватностью. Некоторые из них компании в открытом письме задал главный прокурор штата Коннектикут. В 2013 г. он же заставил Google внедрить правила проверки приложений для очков дополненной реальности Google Glass.

Главный прокурор американского штата Коннектикут Джордж Джепсен (George Jepsen) опубликовал открытое письмо к компании Apple, в котором попросил дать ответы на вопросы, связанные с умными часами Apple Watch.

Прокурора, в частности, интересует, где будут храниться персональные данные и данные о здоровье пользователя Watch — в самих часах или на сервере, — и если на сервере — какие меры защиты этих данных будут предприняты. Второй вопрос — будет ли Apple проверять приложения сторонних разработчиков на наличие уязвимостей, которые могут привести к утечке данных пользователей.

Также его интересует, не смогут ли приложения для установления диагноза и рекомендаций для лечения заболеваний навредить пользователям. Джепсен указывает, что такие программы должны соответствовать законодательству в сфере здравоохранения, а у Apple должен быть механизм проверки соблюдения этих законов и медицинских требований.

Наконец, Джепсена интересуют и более общие проблемы: например, какие именно данные намерены собирать Apple и разработчики приложений.

Как сообщили в пресс-службе прокурора, в прошлом году по аналогичной инициативе Джепсена была организована встреча с представителями Google. По ее итогам компанией Google были внедрены правила проверки приложений, разрабатываемых для очков дополненной реальности Google Glass.

«Когда на потребительском рынке появляются новые технологии, непременно возникают новые вопросы, связанные с приватностью, — прокомментировал Джепсен. — На своем опыте я убедился в эффективности взаимодействия, осуществляемого до выхода нового продукта на рынок».

Напомним, что Google даже пришлось заниматься опровержением мифов, окруживших очки Glass. И большинство из этих мифов касались именно приватности.

Apple Watch были представлены 9 сентября вместе с новыми iPhone 6 и iPhone 6 Plus.

Умные часы оснащены цветным сенсорным дисплеем, колесом управления Digital Crown, датчиком пульса, микрофоном и динамиком и работают в тандеме с iPhone. Специально для часов был разработан свой графический интерфейс. Устройство умеет снимать пульс, составлять программы тренировок и понимает голосовые команды. Разрабатывать приложения для Watch можно будет с помощью платформы WatchKit. Apple планирует выпустить новинку в 2015 г. в трех вариантах, включая вариант в золотом корпусе, и с несколькими ремешками на выбор (всего более 28 различных комбинаций).

Между тем, главный прокурор Коннектикута — не единственный, кого беспокоит сохранность данных пользователей Watch. Многие люди задали этот вопрос после презентации Watch. В одном из интервью после анонса генеральный директор Тим Кук (Tim Cook) попытался успокоить общественность. «Наш бизнес основан на продаже продуктов. Наш бизнес не основан на том, чтобы иметь информацию о вас. Вы — не наш продукт», — заявил он.

Добавим, что ответы на некоторые вопросы Джепсена уже есть в обновленных правилах использования платформы HealthKit. В них говорится, что данные о здоровье пользователя не будут храниться в облаке iCloud, а программы, которые попытаются это сделать, будут удалены из магазина. Компания также запретила разработчикам передавать медицинские данные третьим лицам, не получив согласия пользователя.

Глава Apple выступил с заявлением о защите личных данных

18 сентября 2014, США
Источник: vestifinance.ru

Тим Кук, Главный исполнительный директор Apple

Спустя несколько недель после разразившегося скандала, связанного с утечкой фотографий знаменитостей с серверов iCloud, Apple выступила с обращением, в котором рассказала о том, какое внимание компания уделяет безопасности и сохранности данных своих клиентов.

Напомним, от действий киберпреступника, взломавшего аккаунты в облачном хранилище, предположительно, пострадали актрисы Дженнифер Лоуренс, Кейт Аптон, Кирстен Данст, певица Ариана Гранде и другие, всего около ста человек.

Ранее в интервью The Wall Street Journal Тим Кук утверждал, что утечки Apple ID и паролей с серверов компании не было. Хакерам удалось получить доступ к аккаунтам в iCloud через подбор ответов на контрольные вопросы, при помощи которых можно узнать пароль. Злоумышленники также использовали фишинг для определения ID и паролей.

Компания обновила политику конфиденциальности данных, которая опубликована на новом сайте, посвященном этой важной для Apple теме в рамках запуска iOS 8. Кроме того, был выпущен отдельный 43-страничный документ (white paper), поясняющий подход Apple к данному вопросу.

Глава Apple, Тим Кук, также особо отметил важность защиты личной информации для Apple, а также прокомментировал такие насущные проблемы, как запросы со стороны госорганов и изменения в iOS 8, которые позволят еще более усилить защищенность данных.

"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.

Безопасность и конфиденциальность данных являются важнейшими параметрами, которые учитываются при разработке всех наших продуктов, программного обеспечения и сервисов, в том числе iCloud и таких новых услуг, как Apple Pay. И мы продолжаем работать над усовершенствованием наших продуктов. 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.

<<...Компания Apple обновила политику конфиденциальности данных, которая опубликована на новом сайте, посвященном этой важной для Apple теме в рамках запуска iOS 8...>>

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 даем возможность с легкостью изменить настройки для ограничения передачи этих данных, если вы позднее поменяете свое решение. Каждый продукт Apple создан на основе этих принципов. Если мы запрашиваем ваши данные, то делаем это лишь с целью обеспечить наилучший пользовательский опыт.

Мы создали этот сайт, чтобы пояснить, как мы обращаемся с вашей личной информацией, что именно мы собираем или не собираем 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.

Несколько лет назад пользователи различных интернет-услуг начали понимать, что при использовании таких бесплатных сервисов они являются скорее продуктом, чем клиентом. Но в Apple мы считаем, что отличный пользовательский опыт не должен обеспечиваться за счет нарушения конфиденциальности данных.

Наша бизнес-модель очень проста: мы продаем отличные продукты. Мы не собираем досье на пользователей на основе содержимого вашей электронной почты или часто просматриваемых веб-страниц, для того чтобы впоследствии продать эту информацию рекламодателям. Мы не "монетизируем" информацию, которую вы храните на своем 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 все лучше. Вот и все.

Лишь одна очень небольшая часть нашего бизнеса 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.

Наконец, я хочу еще раз заострить внимание на том, что мы никогда не работали ни с одной из государственных структур ни в одной стране над созданием закладок для доступа к данным пользователей в наших продуктах и услугах. Мы также никогда не предоставляли доступа к нашим серверам. И никогда не пойдем на это.

Наша приверженность принципам защиты ваших персональных данных основана на глубоком уважении к нашим клиентам. Мы знаем, что ваше доверие не дается легко. Именно поэтому оно у нас есть, и мы будем продолжать прикладывать невероятные усилия, для того чтобы укреплять и сохранять его."

Adobe закрывает российское представительство

29 сентября 2014, Россия, Москва
Источник: novostiit.net

Российское представительство компании Adobe, ООО "Адоб системс" подало в Федеральную налоговую службу уведомление о ликвидации юридического лица.

Факт закрытия компании изданию также подтвердил и представитель Adobe Матвей Киреев.

По словам Киреева, Adobe находится в процессе полной ликвидации представительства в России, однако пользователи смогут по-прежнему покупать продукты и услуги Adobe через сайт компании и реселлеров.

Неназванный собеседник издания предположил, что закрытие российского представительства Adobe может быть связано с введенными против России санкциями. По его словам, у компании сорвалось в России несколько сделок, а кроме того, Adobe оказалась не готова к вступлению в силу поправок к закону "О защите персональных данных", которые вводят запрет на обработку данных россиян за рубежом.

Впрочем, через некоторое время представители компании опровергли это заявление. "Решение о ликвидации продиктовано нашей бизнес-стратегией и стратегией по управлению рабочей силой и не является свидетельством финансового положения компании в России или за рубежом. Оно также не связано с вопросами безопасности.

Для справки, за период с 2012 года мы сократили общее количество представительств с 80 до 56?, – сообщается в заявлении пресс-службы Adobe, опубликованном на портале "Цукерберг позвонит".

Отметим, что об увольнениях в российском представительстве Adobe стало известно в феврале 2014 года. Тогда штат компании, насчитывающий 20 сотрудников, был сокращен наполовину. Спустя еще месяц компания уволила всех сотрудников, которые занимались борьбой с пиратством в России.

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.

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».

Владимир Уфнаровский, исполнительный директор компании «Ланит-Терком»

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.

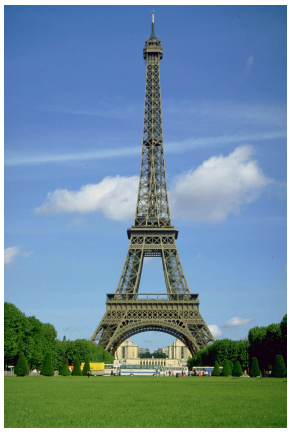
Олег Юдин, руководитель отдела маркетинга компании Artezio отмечает, что любая информация при обмене данными доступна специалистам компании, предоставляющей сервис. «Если вы хотите анонимизированного использования GPS, пользуйтесь им только как приемником сигнала спутников и определения местоположения 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».

Европа по-прежнему рассчитывает на победу в битве за персональные данные

01 октября 2014, Франция
Источник: ridus.ru



В отличие от американского интернет-гиганта Google, французское экспертное сообщество считает, что повышение эффективности оказываемых услуг не оправдывает риска персональными данными пользователей.

Персональные данные пользователей сети Интернет должны быть защищены на национальном уровне. К такому выводу пришли участники Авиньонского форума, прошедшего в Париже. Главной темой форума, проходившего в этом году под названием «100% данных» стала защита персональных данных интернет-пользователей.

Участники Авиньонского форума убеждены, что данные пользователей без достаточных юридических оснований и «в больших количествах поступают на облачные серверы», что повышает риск нарушения права пользователей на невмешательство в их частную жизнь. Об этом пишет французская газета La Croix.

Необходимо позволить каждой стране или континенту принять соответствующие их культуре правила, регламентирующие статус данных, локализацию серверов, шифрование данных и создание суверенной операционной системы, отметили участники форума.

Участники форума также пришли к выводу, что штрафы, установленные благодаря усилиям Национальной комиссии по информатике и свободе, проблему совершенно не решают.

Европейцы оценили свои персональные данные в €240 с человека

01 октября 2014, Великобритания
Источник: telekomza.ru

Потребители телекоммуникационных услуг становятся все лучше осведомлены о ценности своих персональных данных для компаний. Согласно опросу, проведенному оператором Orange в Европе, потребители в среднем оценивают свои персональные данные в 240 евро, что примерно соответствует 12 тыс. российских рублей. Сюда входит их местоположение, различные идентификационные данные, вкусы, демографическая информация.

Правда, опрошенные готовы сделать скидку для тех компаний, с которыми они хорошо знакомы. В этом случае оценка составляет 170 евро.

Orange опросила больше 2000 пользователей мобильных устройств в Великобритании, Франции, Польше и Испании. 80 % из них хорошо знают, что их данные имеют ценность для телекоммуникационных компаний. 67 % считают, что когда люди публикуют свои персональные данные, от этого больше выигрывают компании, чем сами пользователи. Лишь 6 % придерживаются противоположной точки зрения.

«Потребители очень хорошо осознают, что информация о них, которой владеет компания, имеет ценность для этого бренда», -– отмечают исследователи. При этом они признают, что компаниям все сложнее получать такие данные: «Установление и поддержание необходимого доверия, позволяющего организациям извлекать выгоду из передачи, хранения и анализа этих данных, в ближайшие годы станет критически важным новым полем боя для всех цифровых игроков».

Соглашения и партнерства. Сотрудничество. Обмен опытом

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.

Группа компаний «БТП» выходит на сотрудничество с партнёрами из Франции и Германии

03 октября 2014, Россия, Алтайский край
Источник: press-release.ru

11 сентября в Алтайской торгово-промышленной палате в рамках Президентской программы подготовки управленческих кадров состоялась биржа контактов предпринимателей из Франции, Германии и Нидерландов с алтайскими партнёрами. Генеральный директор Группы компаний «БТП» Андрей Басаргин выступил на бирже представителем компании «БТП» и

Ассоциации Обучающих Центров.

Биржа контактов состоялась благодаря Алтайскому региональному ресурсному центру и Алтайской торгово-промышленной палате. Открылось мероприятие заседанием круглого стола, за которым встретились президент Алтайской ТПП Б. Чесноков, директор Алтайского регионального ресурсного центра Р. Моисеев, представители Регионального ресурсного центра, партнёры зарубежных стран и предприниматели Алтайского края. После приветственных слов и выступлений прошли презентации деятельности зарубежных и алтайских компаний. Предприниматели выразили заинтересованность в развитии своего бизнеса в Сибири и провели индивидуальные переговоры.

В рамках презентаций компания «БТП» рассказала о своём опыте в сфере информационно-коммуникационных технологий, представила программные разработки, направленные на повышение эффективности в области государственных закупок, госзаказа, защиты персональных данных. Сервисы находят своё применение в России, Китае, и круг заинтересованных в применении электронных систем «БТП» расширяется.

А. Басаргин принял участие в переговорах с зарубежными партнёрами, в ходе которых представители французской компании «SBM» Игорь Ирик и Гания Мустаев выразили заинтересованность программными разработками компании «БТП», увидев пути расширения рынка сбыта в возможностях информационно-аналитической системы «Фабрика закупок». Инновационная разработка содержит обширную базу о поставщиках, позволяет своевременно проводить анализ данных о заказчиках, поставщиках-конкурентах, отслеживать закупки и многое другое.

В ходе переговоров также были найдены общие интересы Ассоциации Обучающих Центров, в которую входят компании группы «БТП», с коллегами из Германии, представившими Институт психологической интеграции Balance и Агентство экономического развития земли Брандербург. Сотрудничество поможет обменяться опытом проведения семинаров и вебинаров, дополнить обучающие мероприятия и конференции практикой зарубежных экспертов и взаимовыгодно расширить деятельность по организации обучающих мероприятий.

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 рабо-

ты 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.

Персональные данные личности

Автор: Петрыкина Наталья
Издательство: МГИМО-Университет
Год: 2012
Источник: ozon.ru

Настоящее учебное пособие является материалом к курсу "Информационное право России". В нем представлена комплексная характеристика института персональных данных личности, рассмотрены понятие и сущность персональных данных, особенности обработки их различных видов, дана характеристика правовых статусов участников отношений в сфере оборота персональных данных, а также подняты проблемы применения мер юридической ответственности.

Пособие предназначено для студентов юридических вузов.

Обучение / повышение квалификации

Курс "Построение системы безопасности персональных данных в организации"

Период работы: 21.12.2014 - 28.12.2014
Место проведения: Россия, Москва
Организатор - Центр компьютерного обучения «Специалист» при МГТУ им.Н.Э.Баумана,
+7(495)232-32-16
Источник: specialist.ru

Вы — руководитель или специалист информационной службы, IT-подразделения или подразделения по технической защите информации? Вы отвечаете за защиту персональных данных? Тогда курс «Построение системы безопасности персональных данных» именно для Вас!

Необходимость обеспечения безопасности персональных данных в наше время — объективная реальность. Информация о человеке всегда имела большую ценность, но сегодня она превратилась в самый дорогой товар. Безопасность персональных данных обеспечивается и регулируется федеральным законом N 152-ФЗ «О персональных данных», ведь информация в руках мошенника превращается в орудие преступления, в руках уволенного сотрудника — в средство мщения, в руках инсайдера — товар для продажи конкуренту. Именно поэтому персональные данные нуждаются в самой серьезной защите.

Хотите создать в Вашей организации максимально эффективную систему безопасности данных и защитить информационные ресурсы? Пройдите обучение у преподавателей-экспертов в Центре «Специалист». Вы научитесь выполнять требования нормативных правовых актов, руководящих и методических документов по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, а также сможете эффективно планировать и реализовывать комплекс мероприятий по минимизации рисков, связанных с обеспечением безопасности персональных данных в вашей компании.

Курс «Построение системы безопасности персональных данных» вместе с авторизованными курсами Microsoft, курсами SCP, Ethical Hacker входит в одно из наиболее актуальных направлений – «Информационная безопасность». Знания, полученные на курсах этого направления под руководством ведущих специалистов данной сферы, позволят Вам максимально эффективно обеспечить информационную безопасность компании, минимизировав риск потери ценнейшего современного ресурса – информации.

ППК-4ПД: «Обеспечение безопасности персональных данных на предприятии»

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 организаций и их структурных подразделений, в ведении которых находится обработка персональных данных; руководителей и специалистов, отвечающих за обеспечение информационной безопасности предприятий; работников кадровых органов; юристов предприятий-операторов персональных данных; специалистов, реализующих мероприятия по технической защите конфиденциальной информации.

Целевая установка: во время проведения занятий рассматриваются правовые, организационные и технические аспекты обеспечения безопасности персональных данных; на основе изучения требований руководящих документов ФСБ и ФСЭК РФ по обеспечению безопасности персональных данных при их обработке в информационных системах, а также без использования средств автоматизации у слушателей формируется представление о полном цикле и последовательности работ по созданию и обеспечению функционирования системы защиты персональных данных на предприятии.

Содержание программы: общие положения; нормативная правовая база по обеспечению безопасности персональных данных; основные направления деятельности должностных лиц, отделов и служб предприятия по обеспечению безопасности персональных данных; обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных; обеспечение безопасности персональных данных при их обработке без использования средств автоматизации; практические рекомендации; изучение, подбор и расстановка кадров, принимающих участие в обеспечении безопасности персональных данных.

Курс "Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных"

Период работы: 01.12.2014 - 06.12.2014
Место проведения: Россия, Екатеринбург, Уфа, Ростов-на-Дону
Организатор - Учебный центр Softline, +7(495)228-4707
Источник: edu.softline.ru

В ходе курса слушатели изучают правовые и организационные основы обеспечения безопасности в информационных системах персональных данных, методы и процедуры выявления угроз безопасности ПДн и оценки степени их опасности. В рамках практических занятий отрабатываются навыки в проведении мероприятий по обеспечению защиты персональных данных при их обработке в информационной системе персональных данных.

Курс БПД дает исчерпывающую информацию о правовых и организационных основах, методах и процедурах выявления угроз безопасности ПДн, а также оценки степени их опасности. На практических занятиях в рамках данного курса вы отработаете навыки в проведении мероприятий по обеспечению защиты персональных данных при их обработке в информационной системе персональных данных.

Чему вы научитесь: Ориентироваться в иерархии и классах информационной системы персональных данных. Выявлять угрозы безопасности на объектах информатизации, применять организационные меры, технические и программные средства защиты информации от несанкционированного доступа. Анализировать технические каналы утечки информации и противодействовать им. Приводить в соответствие с правовыми и организационно-распорядительными документами в области технической защиты информации системы обработки персональных данных в организации.

Программа курса:

Модуль 1. Безопасность персональных данных. Актуальность тематики.

Модуль 2. Выявление угроз и уязвимостей безопасности персональных данных.

Модуль 3. Организационные и технические меры по обеспечению безопасности персональных данных при их обработке в ИСПДн.

Модуль 4. Процедура приведения ИС в соответствие с требованиями законных и подзаконных актов. Формирование организационно-распорядительной документации.

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 "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.

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.

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

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.

Эмблема СНГ

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

02 октября 1971 (43 года назад)

День рождения электронной почты (Birthday e-mail)

США

Источник: friends-forum.com

Как говорят факты, в 1971 инженер американской компании BBN Technologies Рэй Томлинсон, которому тогда было 30 лет, отправил внутри офиса по локальной сети с одного компьютера на другой первое электронное послание.

К сожалению, текст, который был отправлен в качестве первого электронного письма, не сохранился. Одни утверждают, что ничего осмысленного в нем не содержалось - Рэй просто провел пальцем по верхнему ряду клавиш на клавиатуре, другие говорят, что текст письма содержал отрывок из произведения классика.

Первая программа для отправки сообщений состояла всего из 200 строк программного кода и применялась не в Интернете (такого понятия в 1971 еще не было), а в военной сети ARPA Net. Именно тогда в качестве разделителя между именем пользователя и доменом было предложено иметь символ "@", который у нас принято называть "собакой". Выбор был обусловлен тем, что "@" был редко используемым символом.

02 октября 1992 (22 года назад)

В Украине принят закон "Об информации", регулирующий отношения по созданию, сбору, получению, хранению, использованию, распространению, охране, защите информации

Украина

Источник: online.zakon.kz

Закон Украины от 2 октября 1992 № 2657-XII регулирует отношения по созданию, сбору, получению, хранению, использованию, распространению, охране, защите информации. Основными принципами информационных отношений являются: гарантированность права на информацию; открытость, доступность информации, свобода обмена информацией; достоверность и полнота информации; свобода выражения мнений и убеждений; правомерность получения, использования, распространения, хранения и защиты информации; защищенность личности от вмешательства в ее личную и семейную жизнь.

Основными направлениями государственной информационной политики являются: обеспечение доступа каждого к информации; обеспечение равных возможностей для создания, сбора, получения, хранения, использования, распространения, охраны, защиты информации;создание условий для формирования в Украине информационного общества; обеспечение открытости и прозрачности деятельности субъектов властных полномочий; создание информационных систем и сетей информации, развитие электронного управления; постоянное обновление, обогащение и хранение национальных информационных ресурсов; обеспечения информационной безопасности Украины; содействие международному сотрудничеству в информационной сфере и вхождению Украины в мировое информационное пространство.

04 октября 1990 (24 года назад)

В США создан центр надзора и контроля за преступностью в Internet

США

Источник: prostoy.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, задача которого заключается в проведении контроля за преступностью в Интернет. В его обязанности входит обнаружение атак хакеров в сети и затем оперативное извещение банков и финансовых институтов о наличии угрозы.

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

16 октября 1999 (15 лет назад)

В СНГ принят Модельный закон «О персональных данных»

Россия, Санкт-Петербург

Источник: lawmix.ru

Законом №14-19 государств-участниц СНГ от 16 октября 1999 определяются операции с персональными данными и их правовой режим с учетом общепризнанных норм международного права и обязательств по международным договорам.

Целью Закона является защита прав человека в отношении его персональных данных и операций с ними, определение правового режима использования персональных данных и функций их держателей.

Законом установлено:

- Персональные данные должны быть получены и обработаны законным образом на основании действующего законодательства.

- Персональные данные включаются в базы персональных данных на основании свободного согласия субъекта, выраженного в письменной форме.

- Персональные данные должны накапливаться для точно определенных и законных целей, не использоваться в противоречии с этими целями и не быть избыточными по отношению к ним.

- Персональные данные, предоставляемые держателем, должны быть точными и в случае необходимости обновляться.

- Персональные данные должны храниться не дольше, чем этого требует цель, для которой они накапливаются, и подлежать уничтожению по достижении этой цели или при миновании надобности.

- Должны приниматься меры для охраны персональных данных, исключающие случайное или несанкционированное разрушение или случайную их утрату, а равно несанкционированный доступ к ним, изменение, блокирование или передачу данных.

- Не допускается объединение баз персональных данных, собранных держателями в разных целях, для автоматизированной обработки информации.

- Для лиц, занимающих высшие государственные должности, и кандидатов на эти должности национальным законодательством может быть установлен специальный правовой режим для их персональных данных, обеспечивающий открытость только общественно значимых данных.

16 октября 2000 (14 лет назад)

На 80 страницах отчёта, представленного во французский Парламент Комиссией по обороне, подробно доказано, что все средства коммуникации от факса до телефонной связи находятся под постоянным прослушиванием шпионской сети США под кодовым названием «Эшелон»

США
Источник: ru.wikipedia.org

В первую очередь объектами наблюдения становятся европейские компании, конкурирующие с компаниями США.

В Соединенных Штатах данные просеиваются суперкомпьютерами в поисках ключевых слов и фраз. По результатам расследования, проведенного в 2001 году Европейским Парламентом, "Эшелон" может перехватывать три миллиона факсов, электронных посланий и телефонных разговоров в минуту. От 10000 до 15000 сообщений ежедневно признаются заслуживающими интереса и подлежащими расшифровке и анализу. Суперкомпьютеры "Эшелона" могут даже "взламывать" зашифрованные сообщения. ("The Washington Times", США)

Нарастающий скандал, связанный с прослушиванием членов Совета Безопасности Организации Объединенных Наций перед войной в Ираке, с высокой вероятностью прольет нелицеприятный свет на тайну, которую Вашингтон и Лондон отчаянно пытаются сохранить - на созданную Агентством национальной безопасности США систему электронной разведки "Эшелон". В то время как Австралия и Новая Зеландия признали, что соответствующие соглашения и системы существуют, Вашингтон на все запросы, касающиеся "Эшелона", отвечает немногословной фразой: "без комментариев". В 1999 году член Постоянного специального комитета по разведке Палаты представителей Конгресса США Бобб Барр (Bob Barr) пришел в ярость, когда АНБ, чтобы не предоставлять Комитету запрашиваемые им документы о сверхсекретной системе, заявило о своем праве не разглашать информацию, полученную из своих источников. Система "Эшелон" возникла в 1971 году. АНБ сотрудничает с английской Штаб-квартирой правительственной связи и соответствующими ведомствами Канады, Австралии и Новой Зеландии. Однако радиоантенны, перехватывающие сигналы, располагаются не только на территории этих пяти стран, элементы глобальной сети прослушивающих станций АНБ находятся также в Италии, Турции и даже на островах Эритреи. Разведывательные ведомства других стран также сотрудничают с АНБ, но на двусторонней основе. Пятерка партнеров по "Эшелону" обменивается друг с другом списками имен, мест, ключевых слов и выражений; и когда нужный термин обнаруживается в перехваченном сообщении, то оно сразу же отсылается соответствующей стране.

17 октября 2012 (2 года назад)

ISO представила новый стандарт ISO/ IEC 27032 для обеспечения безопасности онлайн-транзакций

Россия, Москва
Источник: securitylab.ru

Новый стандарт нацелен на ликвидацию недостатков, которые возникают вследствие отсутствия взаимодействия между пользователями и поставщиками услуг в киберпространстве.

Международная организация по стандартизации (ISO) выпустила новый стандарт кибербезопасности, направленый на обеспечение безопасности онлайн-транзакций и личной информации, которой пользователи обмениваются через Интернет. В частности, нововведение ISO будет затрагивать онлайн-торговлю, онлайн-банкинг, цифровые медицинские записи, удаленные офисные приложения и пр.

Эксперты ISO отмечают, что обеспечение безопасности в киберпространстве требует тесного сотрудничества между его составляющими. Новый стандарт нацелен на ликвидацию недостатков, которые возникают вследствие отсутствия взаимодействия между пользователями и поставщиками интернет-услуг.

Нововведение ISO/ IEC 27032 предлагает основу для обмена информацией, координации и управления инцидентами безопасности в интернете. Помимо этого, стандарт предусматривает разработку сайта-связи, который обеспечит безопасное и надежное сотрудничество, предоставляющее защиту цифровой конфиденциальной информации.

Разработчик стандарта Иоанн Амсенга (Johann Amsenga) поясняет, что уязвимости в киберпространстве возникают из-за несогласованности между пользователями и поставщиками услуг.

Положения ISO/IEC 27032 сосредоточены на вопросах обнаружения, мониторинга и реагирования на атаки. В частности, речь идет о методах социальной инженерии, которые применяются при отправке писем электронной почты и других сообщений, о взломанных сайтах, которые распространяют вредоносные и шпионские программы. Помимо этого, определенная часть стандарта разграничивает киберугрозы, которым подвергается конфиденциальная информация пользователей и организаций. В этих рамках будут рассматриваться вопросы по поводу компрометации корпоративной и пользовательской информации.

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.

24 октября 1995 (19 лет назад)

В Европейском союзе приняли Директиву 95/46/EC о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных

Евросоюз
Источник: privacy-info.ru

В соответствии с Директивой Европейского Парламента и Совета Европейского Союза 95/46/EC от 24 октября 1995, государства-участники защищают фундаментальные права и свободы физических лиц, и, в частности, их право на неприкосновенность частной жизни применительно к обработке персональных данных.

Государства-участники не будут ни ограничивать, ни запрещать свободный поток персональных данных между государствами-участниками по причинам, связанным с защитой.

Директивой 95/46/EC устанавливаются:

1) следующие понятия: «персональные данные»; «обработка персональных данных»; «картотека персональных данных»; «контролер»; «обработчик»; «получатель»; «согласие субъекта данных».

2) в каких случаях каждое государство принимает на основании указанной Директивы национальный нормативный акт, регулирующий проведение обработки персональных данных.

3) какие условия должны отражаться в законодательных документах, которые необходимо соблюдать при обработке персональных данных.

4) установлено при каких условиях могут обрабатываться персональные данные. Определено, какую информацию запрещено раскрывать при обработке персональных данных.

30 октября 2007 (7 лет назад)

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

Россия, Москва
Источник: garant.ru

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

Герб Москвы

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.

30 октября 2008 (6 лет назад)

IBM представила устройство для защиты онлайновых транзакций

США
Источник: securitylab.ru

Корпорация IBM разработала компактное устройство, предназначенное для защиты конфиденциальных пользовательских данных во время проведения онлайновых транзакций.

Гаджет с длинным названием Zone Trusted Information Channel создавался специалистами исследовательской лаборатории IBM в Цюрихе (Швейцария). Внешним видом новинка напоминает обычный флеш-брелок, правда, при этом оборудованный небольшим дисплеем.

После подключения к персональному компьютеру через порт USB устройство устанавливает безопасное изолированное соединение с удаленным банковским сервером. Передача данных осуществляется в обход машины пользователя, на которой могут содержаться трояны, вирусы, кейлоггеры и другое вредоносное ПО. Авторизация и необходимые операции со счетом при этом могут выполняться непосредственно через дисплей Zone Trusted Information Channel.

Устройство использует протокол TLS/SSL (Transport Layer Security/Secure Sockets Layer) и поддерживает работу со смарт-картами. При применении новинки не требуется вносить изменения в банковское программное обеспечение; кроме того, упоминается совместимость со всеми распространенными операционными системами.

ПРАВОЧНЫЕ 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 **47345**
Пресса России индекс **38580**
Почта России индекс **99115**

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