

Уважаемые коллеги, заказчики и партнеры!

Предлагаем вашему вниманию взгляд специалистов ИНФОРИОН на ИБ/ИТ-новости января 2011 года.

Как и ранее, мы попытались выделить наиболее яркие и значимые на наш взгляд события прошедшего месяца, снабдив их короткими авторскими комментариями.

С уважением, команда ИНФОРИОН

09.02.2011 г.

«Топ 10» ИБ-новостей и событий

Несмотря на то, что практически всю свою первую половину январь месяц был «выходным», это практически не повлияло на количество событий и новостей в области ИТ/ИБ.

О том, какие события определили начало 2011 года читайте в нашей десятке наиболее значимых новостей в сфере ИТ/ИБ:

1. О детях позаботились

В начале месяца активно обсуждался принятый еще в прошлом году Федеральный закон № 436-ФЗ «[О защите детей от информации, причиняющей вред их здоровью и развитию](#)». Закон вступит в силу с 1 сентября 2012 года и коснется всей информации, размещенной в сети Интернет и не только.

Мнения о новом законе разделились, кто-то называет идею благой и полезной, кто-то недоволен «оторванностью» формулировок от реалий наших дней. Закон и в самом деле получился довольно суровым, но, как он будет работать на практике, покажет только время.

2. Отказ от западных средств

Тем временем «забота» коснулась и свердловских чиновников, которым запретили использовать Skype и бесплатную web-почту в рабочих целях. Кроме того ФСБ России не довольна, что программное обеспечение, средства вычислительной техники и связи в госучреждениях зачастую используются импортного производства, так как это в свою очередь негативно сказывается на состоянии защищенности информации, обрабатываемой с использованием данных средств. Сложившаяся ситуация диссонирует с курсом на широкое распространение ИТ-технологий, установленным президентом РФ, так же стоит отметить, что сравнимых российских аналогов указанных средств практически нет.

3. «Всероссийское генеалогическое древо» под угрозой закрытия

Роскомнадзор решил закрыть известный web-сайт [«Всероссийское генеалогическое древо»](#), который уже 12 лет помогает россиянам изучать свою семейную историю. В судебном иске Роскомнадзор требует признать владельца web-сайта виновным в «нарушении права неопределенного круга лиц на неприкосновенность частной жизни», а также уничтожить генеалогическую базу web-сайта и вообще разделить домен. Заседание суда состоится в ближайшее время, ждем результатов.

4. Слияния и поглощения

В начале месяца компания Dell, [объявила](#) о приобретении западной компании SecureWorks. Это уже не первая сделка Dell в направлении выхода на рынок ИБ, но, как новый игрок собирается завоевывать рынок в условиях уже сформировавшиеся конкуренции, пока загадка.

В середине месяца активно обсуждалась новость о продаже крупного пакета акций компании «Лаборатория Касперского» американскому фонду General Atlantic. Часть своих бумаг продала председатель совета директоров Наталья Касперская. По предварительным данным, представитель фонда войдет в состав совета директоров «Лаборатории Касперского». Крупнейшим акционером компании останется Евгений Касперский, обладающий контрольным пакетом. Наталья Касперская планирует вырученные средства вложить в собственные проекты: Infowatch, «Наносемантику» и «Крибрум».

5. Инсайдерам – нет!

Вступил в силу Федеральный закон № 224-ФЗ [«О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты РФ»](#).

Закон направлен на закрепление системы мер по противодействию неправомерному использованию инсайдерской информации и манипулированию рынком, усиление защиты прав и законных интересов инвесторов.

Документ определяет новые понятия, вводит статьи в УК РФ, закрепляет положения о неправомерном использовании инсайдерской информации, в частности для банков.

Закон вступил в силу с 27 января 2011 года. При этом нормы об административной ответственности будут применяться по истечении 1 года после опубликования закона (с 27 июня 2011 года), а нормы об уголовной ответственности – через 3 года после опубликования закона. Отзыв банковской лицензии у банка, нарушившего закон об инсайте, так же будет введен через 3 года.

6. Снова сдвиг сроков

Сдвиг сроков коснулся не только Федерального закона № 152-ФЗ «О персональных данных», вслед за ним на те же полгода сдвинулся срок уведомления о присоединении к СТО Банка России для кредитно-финансовых организаций – до 30 июня 2011 года.

В [разъяснениях](#) Банка России связь между изменениями в Федеральном законе и переносом срока уведомления указана напрямую.

7. Новые стандарты

Сразу два новых отраслевых стандарта в области обработки персональных данных появились в конце января. Национальная ассоциация участников фондового рынка разработала для своих членов стандарт «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных операторами – профессиональными участниками рынка ценных бумаг», и Национальная ассоциация негосударственных пенсионных фондов (НАПФ) совместно с Leta IT-компану выпустили отраслевой стандарт защиты персональных данных для негосударственных пенсионных фондов (НПФ).

Правда, первый документ доступен только членам НАУФОР, а второму еще предстоит пройти согласование с ФСТЭК России и ФСБ России, но уже сейчас с ними можно ознакомиться на web-сайте [НАПФ](#).

8. Отчеты года

В первый месяц года крупные игроки ИТ-рынка представили отчеты о проделанной работе за 2010 год. Так рост бизнеса Microsoft в России показал увеличение прибыли на 20%, чистая прибыль EMC выросла на 75%, а например, Nokia потеряла часть мобильного рынка по сравнению с 2009 годом. Так же стоит обратить внимание на интересные отчеты [Cisco](#) и [Trustwave](#).

9. Египет ушел в оффлайн

Из-за сложной ситуации в стране на всей ее территории был отключен доступ в сеть Интернет. Все провайдеры друг за другом отключили свои подсети в интервале – 13 минут. Следом были заблокированы sms-сообщения и мобильная связь в целом.

Все мировое ИТ-сообщество обсуждает, должно ли правительство иметь общий «рубильник» на случай чрезвычайных обстоятельств или это противоречит основам демократии.

10. Безопасность после теракта

Теракт в Домодедово повлек за собой громкие отставки и громкие назначения. Президент РФ ввел новую должность замминистра, отвечающего за безопасность на всем транспорте. На эту должность был назначен генерал-полковник милиции Виктор Кирьянов.

В своем первом интервью на новом посту Виктор Кирьянов обозначил своей главной целью выстраивание взаимодействия между ведомствами для более эффективного решения поставленных задач. Значит ли это, что появится единая глобальная система контроля безопасности на транспорте, пока неясно.

Авторская колонка

В последние годы идея организации обработки информации с использованием «облачных» вычислений становится все более популярной. На Западе на них перешел ряд компаний, и значительная часть находится в стадии миграции.

В данной колонке мне хотелось бы затронуть проблемы аутсорсинга с использованием «облачных» технологий. Преимуществом арендуемых «облачных» ресурсов является значительная экономия денежных средств за счет отсутствия необходимости содержать собственные физические ИТ-ресурсы (дата-центры) и иметь обслуживающий их персонал. Компаний, использующих сторонние «облачные» услуги, привлекает высокая масштабируемость и возможность практически мгновенно получить необходимые информационно-вычислительные ресурсы. Особенно это важно в тех случаях, когда большие вычислительные мощности требуются разово.

В России развитие и внедрение данной услуги натолкнулось на несколько проблем. Среди них и отсутствие хороших каналов связи на большей части территории России, и сложность миграции со своих приложений на «облачные», и боязнь отдавать конфиденциальную информацию на аутсорсинг, а также опасения за стабильность работы «облачных» приложений.

Многих потенциальных клиентов «облачных» хостеров все же больше всего волнует вопрос безопасности данных. В «облаке» информация разных организаций находится рядом, на одном физическом сервере, и владелец этих данных не может четко ответить на вопросы, где находятся его данные и кто может получать к ним доступ. Кроме того, зачастую владелец данных не имеет возможности удалить уже неиспользуемые им данные, и ему приходится полагаться на то, что эти процедуры будет выполнять поставщик «облачных» услуг.

Решением проблемы обеспечения безопасности информации при «облачных» вычислениях занимаются крупнейшие ИТ-компании, такие как IBM, MicroSoft, Fujitsu и др. Для изолирования своего виртуального пространства пользователь «облака» может применять виртуальные межсетевые экраны, которые позволяют ему осуществлять фильтрацию трафика и следить за информационными потоками внутри своего виртуального хранилища и на его границах.

Одним из решений вопросов безопасности информации является организация частного «облака», но такой вариант использования «облачных» вычислений доступен только крупным компаниям.

Существует также проблема соответствия информационных систем, использующих «облачные» технологии, требованиям безопасности и методических документах РФ. Так как понятия, связанные с «облачными» вычислениями, законодательно никак не закреплены, то зачастую владелец информации не может предъявить доказательства обеспечения должного уровня защиты обрабатываемых им данных.

Для того, чтобы обеспечение безопасности не вызывало у пользователей «облака» лишних вопросов, технологии, применяемые для обеспечения безопасности данных, должны быть стандартизированы, должна быть внедрена процедура соответствующей сертификации. Тогда клиент, обращаясь к «облачному» провайдеру, будет иметь гарантии обеспечения конфиденциальности, доступности и аутентичности своей информации. Но так как в России практик работы с данной технологией не много, а специализированные стандарты только начинают разрабатываться (причем за пределами России), то «облачным» вендорам приходится убеждать клиентов в безопасности хранения и обработки данных в «облаке» тем, что они используют стандартные алгоритмы шифрования и стандартные средства создания виртуальных машин. Некоторые провайдеры проходят сертификацию на соответствие различным европейским стандартам по безопасности информации, но для российского законодательства такая сертификация не является доказательством обеспечения требуемого уровня защищенности информации.

Таким образом, в настоящий момент «облачные» услуги в России могут быть востребованы небольшими компаниями, которым тяжело содержать собственные мощные серверы, и которые не обязаны отчитываться перед государством о степени защиты обрабатываемой ими информации. Тогда они могут выбрать провайдера, который обеспечивает достаточный, по их мнению, уровень безопасности и пользоваться его услугами. Средние компании, при использовании «облачных» услуг, скорее предпочтут только SaaS (ПО как услуга), отдавая на аутсорсинг антивирусы и почтовые приложения. Крупные же организациям сейчас проще оставаться на своих ЦОДах и серверах, ведь у них уже построены и отработаны бизнес-процессы, а миграция на «облака» будет представлять нетривиальную задачу и в некоторых случаях может стать проигрышной стратегией.

Дарья Муравьева
Специалист отдела проектных работ

Идея: Т. Кузьменко

Материал: А. Иржавский, А. Кузнецов, Д. Муравьева, Т. Кузьменко

При подготовке использованы источники:

www.cbr.ru
www.content.dell.com
www.dkvartal.ru
www.kaspersky.ru
www.lenta.ru
www.napf.ru
www.renesitys.com
www.rg.ru
www.rian.ru
www.rsoc.ru
www.securitylab.ru
www.uinc.ru
www.webplanet.ru
www.allnokia.ru

© ООО ИНФОРИОН, 2011 г.