

Уважаемые коллеги, заказчики, партнеры!

В продолжение аналогичной публикации месячной давности предлагаем Вашему вниманию взгляд специалистов ИНФОРИОН на ИБ/ИТ-новости ноября.

Как и ранее, мы попытались выделить наиболее яркие и значимые на наш взгляд события прошедшего месяца, снабдив их коротким авторским комментарием.

С уважением, команда ИНФОРИОН

06.12.2010 г.

«Топ 10» ИБ-новостей и событий

Предпоследний месяц года был насыщен разнообразными событиями. Выводим за скобки события вокруг WikiLeaks (об этом за последнее время сказано немало, причем – сказано устами ведущих политиков) и предлагаем следующую десятку наиболее значимых (по нашему мнению) новостей в сфере ИТ/ИБ:

1. «Лэндраш» («Золотая лихорадка») или регистрация доменов по-русски

Начавшаяся 11 ноября открытая регистрация доменов в зоне «.рф» закончилась скандалом. Регистратор RU-CENTER был обвинен Координационным центром национального домена сети «Интернет» в киберсквоттинге. При этом, складывается ощущение, что Координационный центр сам допустил столь непростую ситуацию, отказавшись от идеи «премиальных регистраций» тремя месяцами ранее. Спорные имена в зоне «.рф» были «заморожены», RU-CENTER уже было собирался подать в суд на Координационный центр, но к концу месяца сторонам все же удалось договориться, домены были разблокированы. Хочется надеяться, что на этом история закончится.

2. Новые поправки в законодательстве

Готовятся поправки к закону о СМИ. Проект расширит понятие «средство массовой информации» введением нового термина «сетевое издание», причем вводится строгое разграничение между тем, какие ресурсы можно регистрировать, как СМИ, а какие нет. Кроме того, готовятся поправки и в 149-й закон «О защите информации», которые введут уголовную ответственность за рассылку спама. Примечателен проект еще и тем, что документ будет содержать определения таких понятий, как «электронная почта», «доменное имя» и «пользовательский контент», а также законодательно закрепит ответственность за рассылку спама. Ситуация с регистрацией доменов в зоне «.рф», показывает, что введение четких определений и понятий в сетевой сфере и в области массовых коммуникаций отнюдь не повредит.

3. Электронный документооборот теперь по ГОСТу

Приказом Федерального агентства по техническому регулированию и метрологии от 26.10.2010 № 327-СТ утвержден ГОСТ Р 53898-2010 «Системы электронного документооборота. Взаимодействие систем управления документами. Требования к электронному сообщению». Текст документа явно указывает на то, что «порядок применения ЭЦП не является предметом стандарта, а рассматривается как «внешний» по отношению к нему». От комментариев относительно других аспектов нового документа воздержимся, помня универсальную мудрость про то, что даже «слабый» стандарт лучше его отсутствия.

4. Особая версия червя Zeus

О черве Zeus специалисты ИБ знают давно, но в этом ноябре была выявлена его «премиум»-версия, которая работает только на мощных ПК (по оценкам экспертов тактовая частота процессора должна превышать 2 ГГц). Избирательность червя сразу интерпретировали как попытку вредоносной программы формировать ботнеты больших мощностей, но более правдоподобно другое мнение. Дело в излишней «чувствительности» встроенного детектора отладчиков червя, который принимает за исследовательскую среду любой компьютер, частота процессора которого составляет менее 2 ГГц, если значение этого параметра выше, то ВП запускается и работает своим обычным образом, если ниже - активируются процедуры защиты от отладки, исполнение кода прерывается, и операционная система не инфицируется. Складывается ощущение, что вирусописатели просто перестарались.

5. Поправки в закон «О государственной тайне» вступят в силу с 18 февраля будущего года

19 ноября опубликован новый Федеральный закон №299 «О внесении изменений в статью 5 Закона Российской Федерации «О государственной тайне». Перечень сведений, составляющих государственную тайну, дополнен новыми формулировками. Не цитируя дословно изменения, отметим, что они продиктованы тем, что называется «современными вызовами» и находятся в области борьбы с терроризмом и защиты критически важных объектов и потенциально опасных объектов инфраструктуры.

6. Информационное общество 2020

Правительство утвердило программу «Информационное общество» на 2011-2020 гг. Ответственными за ее выполнение назначены Минкомсвязи, Минэкономразвития, ФСО, ФСБ и Минобрнауки. Средства из федерального бюджета уже выделены, так что впереди нас ждет уже не просто электронная Россия, а продвинутое информационное общество и первые места в международных рейтингах. На комментарии должностных лиц, сопровождавшие утверждение программы, очень интересно будет посмотреть спустя 5 – 10 лет, когда должны будут появиться первые значимые результаты «информатизации общества».

7. Mac OS теперь под защитой

«Лаборатория Касперского» выпустила новую версию персонального продукта для Mac OS. Еще пару лет назад понятия «антивирус под мак» просто не было, из-за банального отсутствия образцов компьютерных вирусов для этой операционной системы. Но бурное увеличение числа пользователей подтолкнуло активность вирусописателей. Примечательно, что новый продукт интересен не только пользователям из России, но и зарубежным любителям Apple.

8. Сертифицированное СКЗИ для Oracle с поддержкой российской криптографии

Компания «Аладдин Р.Д.» сертифицировала средства криптографической защиты информации – «Крипто БД», предназначенного для защиты данных в СУБД Oracle от несанкционированного доступа. Решение получило сертификат ФСБ России по классам защиты КС1 и КС2 и стало первым сертифицированным СКЗИ для Oracle с поддержкой российской криптографии.

По словам менеджера по работе с интеграторами «Аладдин Р.Д.» Максима Чиркова разработка продукта велась по договоренности с корпорацией Oracle об использовании российских алгоритмов шифрования в БД. Специалисты ИНФОРИОН считают, что появление такого продукта на рынке ИБ – действительно хорошая новость для крупных интеграторов. Тем не менее, отметим, что еще месяц назад тренеры авторизованных курсов по безопасности Oracle утверждали: служба технической поддержки не отвечает на вопросы, связанные с «прикрученной» к СУБД сторонней криптографией (допускается либо вариант отсутствия криптографии, либо использование «штатных» криптографических средств от самой Oracle).

9. Новая поправка в закон «О персональных данных»

В связи с принятием закона «Об обязательном медицинском страховании в Российской Федерации» Президент подписал Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации». В закон о персональных данных был внесен пункт, дополняющий случаи, когда допускается обработка специальных категорий персональных данных. 152-ФЗ постепенно становится «мягче», но полноценную его работу мы увидим уже меньше, чем через месяц.

Напомним также о том, что анонсирован, но не принят законопроект об очередном переносе времени «Ч» (некоторые операторы в шутку говорят «время «П», наверное, по первой букве термина «Персональные данные»).

10.Международный день защиты информации – 30 ноября

В далеком 1988 году американская Ассоциация компьютерного оборудования объявила 30 ноября Международным днем защиты информации (Computer Security Day). Цель этого Дня — напомнить пользователям и производителям аппаратных и программных средств о необходимости защиты компьютерной информации.

Команда ИНФОРИОН поздравляет всех причастных с праздником! Среди множества тостов, поднимавшихся профессионалами ИБ, отметим золотые слова «за профилактику!»; как известно - профилактика болезни всегда легче ее лечения.

Авторская колонка

Читая новостные сводки о провалах спецслужб и сенсационных публикациях закрытых дипломатических документов США на портале Wikileaks, а также анализируя личный опыт, вновь и вновь приходишь к банальному выводу: слабым звеном любой, даже самой совершенной системы безопасности, по-прежнему остается человек. Тем более поразительно, что именно этому аспекту информационной безопасности по-прежнему уделяется мало внимания со стороны многих заказчиков.

Хотелось бы отметить, что бизнес постепенно отходит от стандартной парадигмы централизованного подхода в управлении; все больше сотрудников различных компаний и учреждений работают удаленно, а значит, их все сложнее и сложнее контролировать, что ведет к проблемам в обеспечении установленного в организации уровня ИБ. Более того, вполне возможно, что количество удаленных сотрудников будет расти значительно быстрее и в нашей стране. Например, в рамках неравной борьбы с пробками в Москве и других крупных городах вполне возможен постепенный дрейф от аренды офисов и создания постоянных рабочих мест в них к увеличению числа надомных работников. Бизнес сам стал активно продвигать идею надомной работы, что продемонстрировал Российский союз промышленников и предпринимателей, предложив свою законодательную инициативу о дистанционной работе¹, которая обсуждалась весь ноябрь (правда, нужно заметить, что в большей степени обсуждение касалось темы увеличения рабочего дня, но и вопрос о дистанционной работе также часто дискутировался).

Вторым важным трендом, указывающим на необходимость более плотной работы с сотрудниками компаний в части информирования и обучения в области информационной безопасности, является обилие социальных сетей, как российских, так и иностранных, что опять приводит к тому, что сотрудники уже вне рабочего места потенциально способны разгласить конфиденциальную информацию, умышленно или непреднамеренно.

Есть и другие факторы, свидетельствующие о том, что в результате эволюции бизнеса и ИТ-систем сегодня, как никогда, основным аспектом обеспечения безопасности должны стать люди, и здесь единственно возможным подходом становится каждодневная кропотливая работа по информированию, обучению сотрудников, в том числе и по вопросам личной безопасности в современном информационном мире².

Опыт проведения тренингов по вопросам ИБ для рядовых и не очень сотрудников организаций-заказчиков показывает, что попытка донести до персонала все азы защиты информации (на уровне пользователей) и особенно правил безопасной работы в корпоративной сети порождает вполне здоровый интерес со стороны аудитории и занятие в своей заключительной стадии (на слайде «Ваши вопросы?») часто переходит в эмоциональный брифинг, где проблемы ставятся, что называется, «от сохи».

Это бесценная практика, и она позволяет значительно повысить качество работы, обращая особое внимание не на общие, а на конкретные и актуальные проблемы обеспечения ИБ в отдельно взятой отрасли, компании, системе. Но чтобы получить подобный опыт, необходимо построить семинар таким образом, чтобы люди не дремали под монотонный голос спикера, а буквально ловили каждое слово и примеряли излагаемую ситуацию на себя. Ключевым фактором для этого являются практические примеры с разбором конкретных (имевших место или потенциально возможных) ситуаций.

Мораль? Заинтересуйте человека, покажите ему, что вопросы ИБ касаются его лично – и результат окажется неожиданно полезным. Для всех.

Кирилл Солодовников
Заместитель начальника отдела
проектных работ

¹ <http://www.rspp.ru/simplepage/2>

² Про средства обеспечения ИБ тоже не забываем, но это не тема данной колонки



107023, г. Москва, ул. Большая Семеновская, 45
тел.: +7 (495) 730-74-88 факс: +7 (495) 984-74-89 <http://www.inforion.ru>

Идея: Т. Кузьменко

Материал: А. Иржавский, К. Солодовников, Т. Кузьменко

При подготовке использованы источники:

www.aladdin-rd.ru
www.anti-malware.ru
www.cctld.ru
www.computersecurityday.org
www.cybersecurity.ru
www.globalcio.ru
www.kaspersky.ru
www.kremlin.ru
www.lenta.ru
www.nic.ru
www.rg.ru
www.rian.ru
www.rsoc.ru
www.rspp.ru
www.rucio.org
www.securitylab.ru
www.uinc.ru

© ООО ИНФОРИОН, 2010 г.