



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

Уважаемые коллеги, заказчики и партнеры!

Предлагаем вашему вниманию взгляд специалистов ИНФОРИОН на ИБ/ИТ-новости мая 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

03.06.2011 г.

«Топ 10» ИБ-новостей и событий

Преддверие лета было настолько насыщенным в плане событий, что сформировать всего лишь десятку было трудной задачей, но мы справились. То ли жаркая погода так повлияла, то ли грядущая пора отпусков явилась естественным стимулом к развитию событий, в любом случае, «горячая» подборка наиболее значимых новостей в сфере ИТ/ИБ перед вами:

1. Новый закон о лицензировании

В начале мая был принят ФЗ-99 «[О лицензировании отдельных видов деятельности](#)». Касательно ИБ произошло два серьезных изменения: все лицензии теперь бессрочные, а лицензий на деятельность, связанную с защитой информации криптографическими методами, стало вместо четырех одна.

Сам закон вступает в силу 3 ноября 2011 года, так что еще есть время изучить все детали. Однако, самой долгожданной поправки в отношении отсутствия необходимости получения лицензии для собственных нужд, за исключением технического обслуживания СКЗИ, так и не появилось.

2. Регистрация на портале госуслуг теперь в разы быстрее

Ростелеком начал продажи USB-ключей с электронной цифровой подписью (ЭЦП) для авторизации на портале [госуслуг](#). Стоимость такого ключа составляет 660 рублей, а его использование позволит получить аккаунт на портале мгновенно. Напомним, что раньше для прохождения регистрации необходимо было заполнить ряд анкет, дождаться подтверждающих кодов по электронной почте, по sms и по Почте России.

Авторизация на портале позволяет заполнять электронные заявления для «действующих» услуг и получать их не выходя из дома.

3. ГЛОНАСС-смартфон

Официально поступил в продажу давно обещанный Владимиру Путину первый смартфон с поддержкой отечественной системы навигации ГЛОНАСС – [МТС 945](#), правда, в реальной продаже его найти не удалось. По заявлению производителя данного устройства китайской компании ZTE МТС заказал у них только пробную партию из 50 смартфонов, этим же объясняется и низкое качество аппарата.

Удручает и цена гаджета, за свое устройство производители хотят не меньше 10 тысяч рублей.

4. ГОСТ 28147-89 взломан?!

В середине месяца появилась шокирующая новость том, что наш ГОСТ 28147-89, который Россия собирает сделать международным стандартом шифрования, взломан!

Тем временем мнения специалистов на счет истинности этой новости разделились. Кто-то считает, что теоретически алгоритм скомпрометирован, но технически на его взлом не хватит ресурсов, которыми человек располагает в настоящее время, а кто-то склонен считать такие заявления попытками помешать планам России потеснить ныне применяемый AES.

Подробный разбор полетов читайте в нашей авторской колонке «Взломан» ГОСТ 28147-89 – конец света уже наступил?»

5. «Яндекс» вышел на IPO

В этом мае компания «[Яндекс](#)» вышла на международный рынок. Начальная цена акций составила 35 долларов за акцию, но сразу после открытия рынка поднялась на 40 %.

IPO «Яндекса» было одним из самых успешных среди российских медийных компаний за последнее время, вся компания была оценена примерно в 11,2 миллиарда долларов. Акции котируются под тикером YNDX.

6. Новый директор ФСТЭК

В конце мая указом президента России Дмитрия Медведева был освобожден от должности директор Федеральной службы по техническому и экспортному контролю (ФСТЭК) Сергей Григоров и назначен на этот пост его бывший заместитель Владимир Селин.

Скорее всего, отстранение от должности прежнего руководителя связано с приближающимся пенсионным возрастом Григорова, а приход его преемника вряд ли изменит курс организации.

7. Штрих-код в паспорте

Согласно новому постановлению Правительства от 27 мая 2011 г. «О машиночитаемой записи в паспорте гражданина Российской Федерации» с 1 июля 2011 г. граждане РФ будут получать паспорта, содержащие заполненную зону машиночитаемой записи. Старые паспорта будут действительны в соответствии с уже существующим законодательством.

Но вот будет ли это штрих-код или все же что-то читаемое и для человека, пока не известно.

8. Новая роль Совета Безопасности

Дмитрий Медведев [подписал](#) указ «Вопросы Совета Безопасности Российской Федерации», который актуализировал и уточнил роль Совета Безопасности РФ. СовБез [является](#) головной структурой, определяющей политику и стратегию России в области ИБ, кроме того Президент поставил перед участниками совета вопрос об организации добровольных пожарных формирований с целью не допустить повторения ситуации прошлого лета, соответствующий указ об этом тоже был подписан.

9. Лидеры российского рынка интеграции в области ИБ

В начале месяца активно обсуждалась статья, опубликованная на anti-malware.ru, посвященная исследованиям российского рынка системной интеграции в области информационной безопасности. Сам жанр таких публикаций – дело неблагодарное, в адрес аналитиков был высказан ряд замечаний со стороны комьюнити. Тем не менее, [отчет](#) вполне себе отражает состояние дел на рынке ИБ. Так лидером рейтинга была названа компания «Ай-Теко», далее «Астерос», «ДиалогНаука», «Информзащита», «Инфосистемы Джет», «Leta Group», «Крок», «Техносерв», «ЭлвисПлюс» и «Энвижн Груп».

10. Новый скандал вокруг «РосПила»

Депутат Госдумы РФ от «Единой России» Павел Зырянов направил в Генпрокуратуру запрос с просьбой проверить логотип антикоррупционного сайта «РосПил» на предмет надругательства над гербом России.

В Уголовном кодексе РФ есть статья 329 «Надругательство над Государственным гербом Российской Федерации или Государственным флагом Российской Федерации» с наказанием в виде ограничения свободы на срок до 2 лет, либо арест на срок от 3 до 6 месяцев или лишение свободы на срок до 1 года.

18 мая экспертиза признала логотип «РосПила» надругательством над гербом России, вследствие чего планируется возбудить дело по статье 329 УК РФ.

Авторская колонка

«Взломан» ГОСТ 28147-89 – конец света уже наступил?

В этом месяце Интернет-общественность узнала о «взломе» блочного алгоритма шифрования, описанного ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». По заявлению известного исследователя и основоположника алгебраической криптографии Никола Куртуа в скором времени появятся публикации, которые развеют миф о стойкости российского, а точнее сказать советского, криптоалгоритма.

Сразу бы хотелось пояснить, что означает «взломан» – это говорит о том, что на основе анализа криптоалгоритма установлена возможность дешифрования зашифрованного текста путем более оптимальным, чем полный перебор криптоключей.

Простыми словами алгоритм содержит уязвимость, т.е. если алгоритм сравнить с серийно-выпускаемым замком, а криптоключи с обычными ключами, то чтобы открыть замок путем полного перебора потребовалось бы последовательно использовать все возможные ключи, но в данном случае для замка «типа ГОСТ» нашлась отмычка. Хотя стоит обратить внимание, что официально «отмычка» еще не опубликована, а также не сказано какой тип атаки использовался (ciphertext-only attack, known-playntext attack, chosen-plaintext attack или другой).

Эта новость не привлекла бы к себе столь острого внимания, если бы не одно но, требования нормативно-правовых и методических документов в области защиты информации ограниченного доступа, в том числе персональных данных, настоятельно рекомендуют, а местами обязывают, использовать только сертифицированные средства криптографической защиты информации (СКЗИ), реализующие ГОСТ алгоритм.

Многие компании, приводящие свои информационные системы в соответствие требованиям действующего федерального законодательства, столкнулись теперь не столько с проблемой доверия процедуре сертификации, т.е. прохождения сертификационных испытаний с целью получения заветного сертификата, а с проблемой гарантий реальной безопасности от применения СКЗИ с реализацией ГОСТ алгоритма.

Но так ли все плохо на самом деле?

Давайте взглянем на западные, на первый взгляд образцовые криптоалгоритмы, которые

используются практически во всех программных продуктах:

- RC5 (продукт Zserver) – «взломан» в 1997 году;
- DES (продукты Oracle) – «взломан» в 1998 году.

Стоит обратить внимание, что здесь мы не затрагиваем вопросы качества создания криптоключей, которые не менее важны стойкости самого криптоалгоритма.

А теперь посмотрим, что мы знаем о ГОСТ алгоритме.

ГОСТ алгоритм был спроектирован для обеспечения военного уровня безопасности на 200 лет вперед. Большинство ведущих экспертов, изучавших ГОСТ, приходили к соглашению о том, что «несмотря на значительные криптоаналитические усилия на протяжении 20 лет, ГОСТ 28147-89 все еще не взломан».

ГОСТ алгоритм был стандартизирован в 1989 году и впервые стал официальным стандартом защиты конфиденциальной информации, но спецификация шифра оставалась закрытой. В 1994 году стандарт был рассекречен, опубликован и переведен на английский язык. По аналогии с AES (и в отличие от DES), ГОСТ 28147-89 допущен к защите секретной информации без ограничений, в соответствии с тем, как это указано в российском стандарте.

В связи с международной стандартизацией в области шифрования ГОСТ 28147-89, которая началась в 2010 году, нам предстоит прочитать еще ни одну статью о попытках атак и взломов нашего стандартна западными криптоаналитиками.

Хочется отметить, что попытка получения информации путем ее дешифрования далеко не самый простой, дешевый и быстрый в реализации подход, и большинству злоумышленников он физически недоступен. Злоумышленникам гораздо проще подкупить сотрудника компании и/или внедрить backdoor посредством вредоносной программы.

В связи с этим хочется отметить, что криптографическая подсистема защиты информации далеко не самая уязвимая в комплексной системе защиты информации, и наши стандарты в данной области абсолютно не уступают западным.

Алексей Федоров
Инженер по безопасности ИС

Идея: Т. Кузьменко

Материал: А. Кузнецов, А. Федоров, Т. Кузьменко

При подготовке использованы источники:

www.anti-malware.ru

www.cnews.ru

www.consultant.ru

www.gosuslugi.ru

www.kremlin.ru

www.lenta.ru

www.lukatsky.blogspot.com

www.price.ru

www.rg.ru

www.rian.ru

www.rospil.info

www.rsoc.ru

www.scrf.gov.ru

www.securitylab.ru

www.uinc.ru

© ООО ИНФОРИОН, 2011 г.