информационно-деловой
ВЕСТНИК
ПАО ЦНПО «КАСКАД»
Качество - достойное Державы!

www.kaskad.ru vestnik@kaskad.ru Издается с 2005 года сентябрь 2015 № 9 (126)


Развивать скрытые резервы!
АКТУАЛЬНО


Чем опасны «закладки»?
ТЕХНОЛОГИИ


Подразделение РЭБ продемонстрировало высокую готовность
НОВОСТИ


Основные угрозы в области информационной безопасности
РЫНОК

ТЕМА НОМЕРА: Импортозамещение

АКТУАЛЬНО

Развивать скрытые резервы!

24 сентября в ПАО ЦНПО «КАСКАД» назначен новый генеральный директор. «Вестник…» всегда уделял пристальное внимание назначениям такого уровня. Не стал исключением и этот раз. На момент беседы Вадим Николаевич находился в должности всего несколько дней, однако уже достаточно хорошо изучил обстановку и любезно согласился ответить на вопросы нашего корреспондента.

В.: Новый человек на таком месте — это всегда новые подходы. Вы уже ознакомились с работой предприятия, есть ли что-то, что хотелось бы изменить?

В. М.: ЦНПО «КАСКАД» — стабильное предприятие со своими традициями, и, конечно же, за то короткое время, что я нахожусь на посту генерального директора, трудно сделать какие-то однозначные выводы. Тем не менее есть вещи, которые можно было бы изменить и, как мне кажется, следует изменить уже сейчас. Прежде всего необходимо провести ряд административных преобразований, повысить качество планирования, чтобы набранный в начале года пакет заказов подвергался минимальной корректировке в процессе их исполнения. Некоторые организационно-технические документы согласуются несколько месяцев. Я думаю, этот процесс можно значительно оптимизировать, в том числе и внутри предприятия. Это позволит подойти к самой производственной работе более сбалансированно. Пока же основной объем работ приходится на конец года, а это вызывает известные трудности, когда все наши специалисты — видите, я уже говорю «наши» — могут разом оказаться в командировках, а география «КАСКАДА» весьма обширна.

В.: Вы намерены расширить эту географию?

В. М.: Не столько географию, сколько задачи, которые мы решаем в тех или иных уголках страны. Сегодня существует очень большой объем работ по космодрому «Восточный». «КАСКАД» присутствует на «Восточном», но мне представляется, это присутствие можно значительно расширить. Встанет ли вопрос о создании там филиала по аналогии с Мирным — покажет время, возможно, этого и не потребуется. Могу сказать как человек, сам работавший на «Восточном»: строительные объемы там огромные, а регион испытывает дефицит квалифицированных рабочих рук. В этих условиях компания, хорошо зарекомендовавшая себя, имеющая законченный цикл по созданию систем (от разработки рабочей конструкторской документации, поставки и монтажа оборудования до испытаний и авторского надзора за эксплуатацией), конечно, выигрывает. «Восточный» сейчас главная космическая стройка страны, и возможности проявить себя там открываются большие — как для компании, так и для отдельного человека.

В.: Сегодня много говорится о кризисных явлениях в экономике. Разумеется, «КАСКАД» не находится в вакууме и никогда не находился: все переживается вместе со страной. Ожидаете ли вы каких-либо проблем с этой стороны?

В. М.: Кто-то говорит «проблема», а кто-то говорит «возможность». В связи с кризисом встает такая важная тема, как импортозамещение. Отечественная наука всегда успешно конкурировала с зарубежной. Да вот хотя бы в вашем последнем номере подробно рассказывается об участии «КАСКАДА» в создании советского цветного телевидения. Тогда мы были на равных с развитыми странами Европы. Сегодня не секрет, что значительная часть электронных компонентов аппаратуры — как собственно космической, так и обеспечивающей наземную инфраструктуру — импортного производства. Это серьезная проблема, но предприятиям типа «КАСКАДА», обладающим достаточными научно-производственными возможностями, вполне по силам ее решить. Частично она уже решается, когда мы изменяем схемы под отечественные компоненты. Это требует согласований, определенной административной работы, но инженерно задача решаема, причем без каких-то вложений и перестроек.

В.: Вы работали в системе Роскосмоса. Приходилось ли сталкиваться с работами «КАСКАДА» раньше?

В. М.: С работами — да, но о том, что многие из них делал именно «КАСКАД», я узнал только сейчас. Мне представляется, предприятию стоит сконцентрировать внимание на конечном продукте. В «КАСКАДЕ» достаточный научный потенциал, чтобы представлять на рынок готовые ОКР. Нам вполне по силам собрать перспективных молодых ребят, подобных нашему главному конструктору, и очень серьезно заявить о себе именно как о разработчике, о поставщике наукоемкого продукта, а это предполагает качественно иные отношения с заказчиками. Время требует от нас четких, ясных и прозрачных решений. И мы готовы их предложить.

Продолжение на стр. 2

АКТУАЛЬНО

Развивать скрытые резервы!

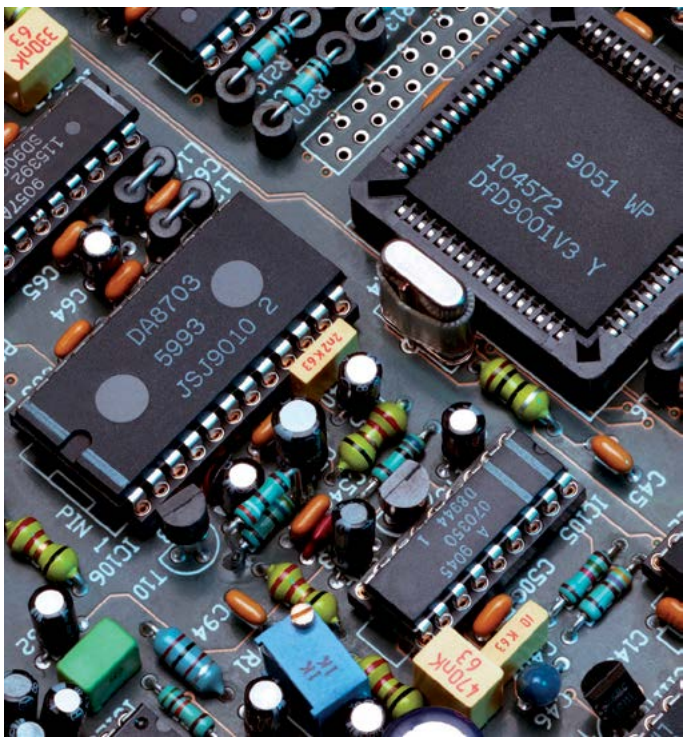
Начало на стр. 1

Митин Вадим Николаевич
Родился 26 августа 1977 года в Москве.
Женат. Двое детей.
Образование высшее, окончил в 2002 году МГТУ им. Баумана по специальности «приборы и системы ориентации, стабилизации и навигации».
С октября 2001 года по август 2008 года работал в ФГУП «ЦЭНКИ» в должности от ведущего специалиста до начальника отдела по техническому и авторскому надзору за вооружением и военной техникой. Занимался разработкой технических заданий и организацией работ по обеспечению пусков РКН с космодромов Байконур и Плесецк, модернизацией технического комплекса на пл. 112 на космодроме Байконур под РН «Союз-2», разрабатывал годовые планы и организовывал работу по обслуживанию, ремонту и доработкам систем и комплексов на космодроме Плесецк, отвечал за государственные контракты с космическими войсками по техническому и авторскому надзору.
С августа 2008 года по сентябрь 2011 года работал начальником отдела эксплуатации космодромов, охраны труда, промышленной и экологической безопасности — заместителем начальника управления средств выведения, наземной космической инфраструктуры и кооперационных связей в Федеральном космическом агентстве. Планировал и организовывал ОКР по модернизации объектов космодрома Байконур, а также мероприятия по их содержанию в рамках Федеральной космической программы на 2006–2015 годы. Участвовал в работах по созданию КРК «Союз-2» в Гвианском космическом центре (Куру), возглавлял комиссию по проведению комплексных испытаний стартового комплекса. Участвовал в государственных комиссиях по пускам РКН с космодромов Байконур и Плесецк. Принимал участие в работах балансовых комиссий подведомственных Роскосмосу предприятий и являлся председателем совета директоров на предприятиях ракетно-космической отрасли. Организовывал работы по экологическому сопровождению пусковых работ на космодроме Байконур совместно с представителями республики Казахстан. Принимал участие в работах по формированию мероприятий в Федеральную космическую программу на 2006–2015 годы по созданию космодрома «Восточный».
С 2011 года по настоящее время работал начальником Центра по созданию космодрома «Восточный», первым заместителем технического директора по космодрому «Восточный» ФГУП «ЦЭНКИ». Возглавлял рекогносцировочные комиссии по размещению комплексов на космодроме, а также трассовых измерительных пунктов. Участвовал в общественных экологических слушаниях в Амурской области. Отвечал за общую координацию ОКР ФГУП «ЦЭНКИ» по созданию систем и комплексов на космодроме «Восточный» и др. Возглавлял рабочую группу по формированию мероприятий по космодрому «Восточный» в Федеральную целевую программу «Развитие российских космодромов на период с 2016 по 2025 год».

ТЕХНОЛОГИИ

Чем опасны «закладки»?

До распада СССР закупка вооружений или хотя бы каких-то компонентов за рубежом практически полностью исключалась, но в 1990-е в производстве стали постепенно использовать импортные компоненты. Вся электроника, используемая в интересах Минобороны и других подобных ведомств, перед ее установкой проходит тщательные проверки Федеральной службы безопасности и специализированных предприятий. Однако 100%-ную гарантию безопасности может дать лишь собственное производство.



«Закладки» — это заложенные в конструкцию какого-либо изделия вредоносные компоненты, которые сложно обнаружить и которые могут быть активированы противником при определенных условиях, например, во время войны. Чтобы избежать их появления в российском оружии, нужно либо тщательно проверять импортные детали, либо самостоятельно проектировать микросхемы и компонентную базу. В таком случае российские инженеры проектируют тот или иной процессор, а затем просто заказывают его производство в том же Китае (производить электронные компоненты в России практически нерентабельно и очень дорого). При этом внесения изменений в конструкцию чипа никто не опасается — нужно быть гением реверс-инжиниринга, чтобы спрятать «закладку» в архитектуре чужого процессора.
Американские военные «закладок» практически не опасаются. Все дело в том, что необходимые микропроцессоры, платы и электронные компоненты проектируются и производятся (причем и в Китае тоже) американскими компаниями или предприятиями стран-союзников. По этой причине Пентагон смело закупает электронику у Intel, Dell, HP, Apple или Samsung. Закупаемая у них продукция должна соответствовать военным стандартам — MIL-STD. Если речь идет о компьютерах, то требуется соответствие требованиям стандартов FIPS-140, MIL-STD-810, MIL-STD-461 и MIL-S-901D. Эти нормативы описывают, как именно электроника должна функционировать в условиях жара и холода, тумана и ледяного дождя, на суше и на воде, в покое и при сильной тряске от взрывов.
Именно поэтому в американских военных компьютерах совсем не редкость — процессоры Core 2 Duo, Core 2 Quad или Xeon, оперативная память Samsung, NEC, Hitachi или Toshiba и операционные системы Windows 98, Windows XP или разные версии Linux, включая SELinux. При этом в последние два года военные стали чаще использовать и миниатюрные портативные устройства — легкие планшеты Samsung или Apple. Правда, программное обеспечение в таких устройствах либо сильно урезано, либо имеет ограничение на использование программ.
Армия США использует ноутбуки Dell как в полевых операциях, например, для получения сведений о местонахождении бойцов, связи или управления беспилотниками, так и в составе командных пунктов. К слову, последние в ближайшее время могут стать беспроводными. Осенью 2015 года военные покажут на армейском форуме беспроводной вариант командного пункта: компьютерная сеть в нем может быть развернута в считанные минуты (против нескольких часов в проводном). Вместо километров кабелей пятой и шестой категории в таких пунктах появятся Wi-Fi-роутеры. Подробности пока неизвестны, но вряд ли это будут специализированные устройства. От обычных потребительских роутеров они, вероятно, будут отличаться только прошивкой, функции которой сократят до минимума в угоду безопасности.

новости

Каждая восьмая утечка информации приходится на сферу гостеприимства

По данным аналитического центра Falcongaze, сфера гостеприимства постоянно подвержена повышенной опасности утечки информации. Почему гостиницы и турфирмы так привлекательны для злоумышленников? В базах данных таких компаний хранится огромное количество информации об адресах, платежеспособности и личности их клиентов.

Гостиницы и туристические фирмы — одни из основных источников краденых номеров кредитных и дебетовых карт. Обычно их системы безопасности защищены не так хорошо, как, например, у предприятий в финансовом и страховом секторе, поэтому в глазах злоумышленников они являются более уязвимой целью.

Один из первых громких случаев массовой утечки персональных данных был связан как раз с похищением информации в сфере гостеприимства. В 2006 году были скомпрометированы данные 234 000 пользователей сайта Hotels.com. А в мае 2015-го были взломаны системы казино и отеля Hard Rock в Лас-Вегасе. Преступники получили доступ к информации о банковских картах посетителей заведения. На протяжении пяти месяцев вредоносное ПО находилось в системе и незаметно «сливало» данные злоумышленникам.

На данные о платежных картах приходится в среднем 90 % от общего количества всей украденной информации. В последние годы эта цифра уменьшается, однако вероятность утечки лишь растет. Если раньше для получения таких данных злоумышленники использовали скимминг, то есть похищали данные непосредственно с терминалов и платежных устройств, то в связи с массовым переходом на пластиковые карты с чипом им приходится применять другие способы. Одним из таких способов как раз и является получение доступа к платежным данным жертв через сервисы сферы гостеприимства.

Амурский университет будет готовить кадры для космодрома «Восточный»

Амурский государственный университет (АмГУ) стал одним из победителей конкурса «Новые кадры для ОПК»: вуз получил по гранту 48 млн рублей на подготовку специалистов для космодрома «Восточный».

Амурский государственный университет стал победителем конкурса проектов Министерства образования и науки РФ по подготовке кадров для оборонно-промышленного комплекса в подведомственных образовательных организациях высшего образования «Новые кадры ОПК». Объем гранта, выделенного на повышение качества подготовки кадров для оборонно-промышленного комплекса, составит 48 млн рублей в 2015–2017 годах, говорится в сообщении.

Уточняется, что организацией-партнером АмГУ является федеральное государственное унитарное предприятие «Центр эксплуатации объектов наземной космической инфраструктуры» (ФГУП «ЦЭНКИ»).

На базе АмГУ создадут новое подразделение — Многофункциональный образовательный центр по подготовке высококвалифицированных кадров для эксплуатации космодрома «Восточный», в состав которого войдут базовая кафедра «Системы наземной космической инфраструктуры» (ФГУП «ЦЭНКИ») и информационно-аналитическое управление реализации образовательных программ для кадрового обеспечения объектов инженерной инфраструктуры космодрома. Специалистов будут готовить в сфере электро- и теплоэнергетики, в области математического и программного обеспечения информационных систем, в сфере охраны труда и техники безопасности. Всего в 2015–2017 годах подготовят 20 студентов-старшекурсников.

В конкурсе «Новые кадры ОПК — 2015» участвовали 75 организаций высшего образования из разных регионов России. Кроме АмГУ среди победителей еще девять вузов.

Сообщается, что всего в рамках конкурса в 2015–2017 годах будет обучено 3000 студентов, предусмотрено государственное финансирование в размере 758 млн рублей. Остальные средства предоставят заинтересованные организации ОПК.

Российские приборы применят в первом проекте ESA по изучению Меркурия

Новостные агентства сообщают, что на межпланетной станции BepiColombo, разработанной специалистами Европейского и Японского космических агентств (ESA и JAXA) для изучения Меркурия, в 2017 году будут установлены российские приборы.

«Российские приборы используют в первом японо-европейском проекте по изучению Меркурия BepiColombo», — говорится в материалах Института космических исследований (ИКИ).

В свою очередь, представитель ESA Альваро Хименес, выступая на конференции в честь 50-летия ИКИ, заявил, что первая японо-европейская миссия, посвященная изучению Меркурия (BepiColombo), очень амбициозна и сложна. «Ее начало запланировано на 2017 год. Она представляет для нас особый интерес, поскольку эта планета аномальна по сравнению с другими планетами Солнечной системы», — сказал он.

Подразделение РЭБ продемонстрировало высокую готовность

В ходе учений войск ЮВО отрабатываются приемы ведения радиоэлектронной борьбы. Так, подразделение радиоэлектронной борьбы ЮВО на полигоне «Нагвалоу» в Абхазии приняло участие в практической отработке задач радиоподавления средств связи и навигации условного противника.

Согласно сообщению, поступившему от пресс-службы Южного военного округа, в ходе отработки ряда задач радиоподавления военнослужащие подразделения РЭБ активно применяют беспилотные летательные аппараты «Леер-3», автоматизированные станции помех «Житель», комплекс «Борисоглебск-1», а также машину генерации помех средствам сотовой связи «Лава-РП».

В пресс-службе военного ведомства подчеркнули, что военнослужащие подразделения РЭБ также осуществили сбор и обработку разведывательной информации на основе приема электромагнитного излучения КВ- и УКВ- диапазонов и посредством генерации радиопомех подавили систему связи для полевых авианаводчиков и наведения высокоточного управляемого ракетного вооружения «противника».

«Тигр-М» МКТК РЭИ ПП — машина РЭБ с комплексом «Леер-2»

Объединенная навигационная система Китая и России может сравниться с GPS

Вице-премьер Дмитрий Рогозин сообщил о возможном объединении спутниковых систем навигации Китая (BeiDou) и России (ГЛОНАСС). По его словам, такое объединение и совместное производство чипсетов позволит создать навигационную систему с очень точным сигналом.

Вице-премьер считает, что подобная система сможет к 2020 году догнать американскую GPS и будет полностью сопоставима с ней по точности сигнала.

Точность калибровки будущей объединенной системы, по словам Рогозина, составит примерно 60 см. Также вице-премьер отметил наличие у российской навигационной системы резервных спутников. Четыре таких спутника в данный момент находятся на орбите и готовы в любой момент включиться в работу.

Всемирная спутниковая навигационная система Китая «Бэйдоу» (BeiDou) появилась сразу после американской GPS и российской ГЛОНАСС. Первые навигационные микрочипы, которые могли принимать сигналы BeiDou совместно с американской и русской системами, появились в 2013 году. Именно такими микрочипами в наши дни оснащено большинство новинок на рынке смартфонов.

РЫНОК

Основные угрозы в области информационной безопасности

Участники рынка компьютерной безопасности отмечают, что в последние несколько лет значительного всплеска киберпреступности не произошло. Вместе с тем не будет преувеличением сказать, что большая часть атак и мошенничества в этой сфере остается незамеченной и просто не попадает в сводки.

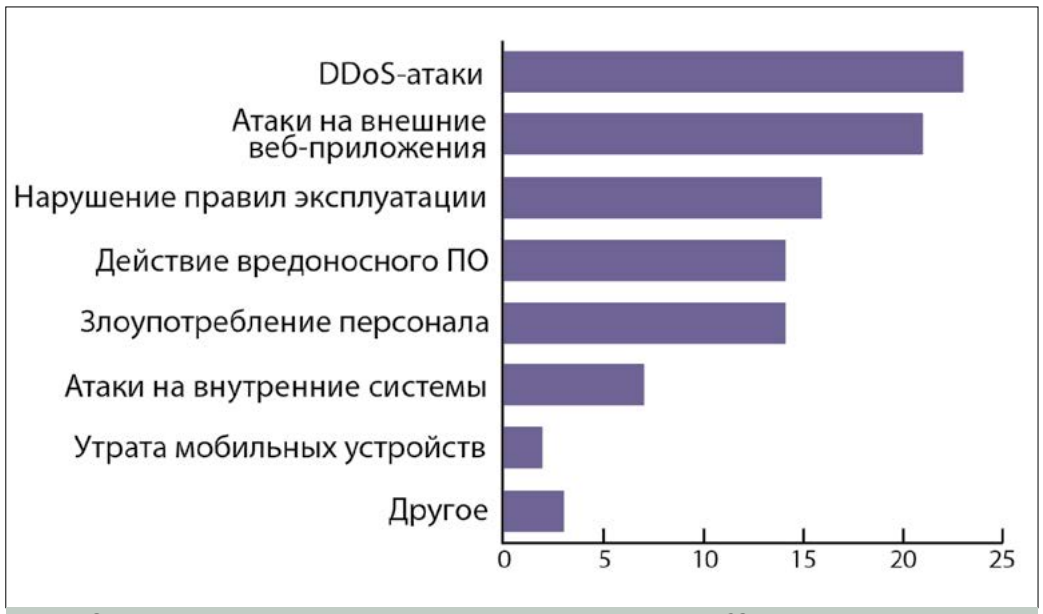


Рис. 1. Основные классы ИБ-инцидентов, с которыми сталкивались в 63 крупнейших российских компаниях

ПАО ЦНПО «КАСКАД» является одним из старейших в нашей стране предприятий, чья деятельность напрямую связана с защитой данных, что подтверждено рядом соответствующих лицензий. Наш опыт говорит о том, что только комплексный подход к вопросам информационной безопасности может дать надлежащий эффект. Это дело профессионалов, однако, чтобы грамотно поставить им задачу, необходимо понимать типы угроз, уметь точно сформулировать проблему.

Основным классом вредоносного ПО остаются бот-сети, которые объединяют зараженные компьютеры в единую инфраструктуру с общим центром управления. Эти средства используются для различных целей: внедрения вредоносного ПО в корпоративные сети, рассылки спама, DDoS-атак. В результате на деятельность, «традиционную» для вредоносного ПО, приходится относительно немного инцидентов (рис. 1).

С бот-сетями ведется активная и весьма успешная борьба. В последние годы целый ряд таких сетей, особенно из числа наиболее крупных, объединивших свыше миллиона зараженных ПК, был деактивирован в ходе операций, которые проводились с участием правоохранительных органов разных стран. Сказываются и конкурентные войны между злоумышленниками, зачастую приводящие к тому, что одна сеть содержит средства, уничтожающие сети, которые принадлежат враждебным группировкам киберпреступников. В результате по итогам 2014 года самая крупная из выявленных бот-сетей насчитывала не более 770 тыс. зараженных узлов. Данная ситуация привела к определенным подвижкам на черном рынке, прежде всего в сфере услуг, связанных с рассылкой спама. Подробнее об этом будет сказано ниже. Вместе с тем злоумышленники компенсировали потери за счет использования других видов оборудования, помимо ПК. Была также преодолена монополия систем на базе Windows. Появлялись, например, сети, целиком состоящие из маршрутизаторов и xDSL-модемов, которые объединяли десятки тысяч устройств. Фиксировалось появление сетей, хотя и меньшего масштаба, из мобильных устройств на базе Android, Mac и Linux, которые долгое время считались не подверженными заражению.

В 2014–2015 годах самыми «модными» остаются целевые атаки. По данным разработчика защитного ПО Symantec, на июнь 2015 года от них больше всего страдали небольшие предприятия с числом работников менее 500 и крупные компании, имеющие свыше 2500 сотрудников: на первые приходилось более 53 % атак, на вторые — более четверти. Среднее время от начала атаки до ее обнаружения превышает 190 дней.

Чаще всего злоумышленники пользуются незакрытыми уязвимостями. Как показывают результаты аудитов ИБ, проведенных компанией Positive Technologies, элементы с такими уязвимостями есть в 90 % корпоративных сетей. Причем ровно половину этих сетей может взломать неквалифицированный злоумышленник или бот, следы деятельности которых обнаруживались даже в процессинговых центрах банков и в биллинговых системах телекоммуникационных операторов. Большого ущерба во многих случаях удалось избежать лишь потому, что злоумышленники просто не поняли, куда попали, и не воспользовались открывшимися перед ними возможностями.

Инструменты кибернападения, как правило, используются для кражи денежных средств или информации, которую легко монетизировать, например реквизитов платежных карт и персональных данных. Средний ущерб от кибератаки в расчете на компанию, по данным исследования «2014 Cost of Cyber Crime Study», проведенного Ponemone Institute, составил 2,3 млн долларов.

За целенаправленными атаками могут стоять и конкуренты. Их цель — всевозможные ноу-хау, информация о готовящихся проектах и новых продуктах, другие сведения, критически важные для бизнеса. Впрочем, эти данные можно похитить и другими способами, в частности с помощью нелояльных сотрудников.

Большой практический интерес к такого рода инструментам проявляют и спецслужбы. Эта категория наиболее коварна и опасна, поскольку за их действиями, скорее всего, стоит не прямой материальный мотив и при этом они обладают значительными ресурсами и квалифицированными кадрами, как собственными, так и наемными. Сюда же можно отнести и деятельность хакеров, которые совершают атаки по идеологическим соображениям, не преследуя материальной выгоды, в отличие от обычных киберпреступников. Впрочем, таких активистов активно используют спецслужбы — или в качестве наемников, или, что называется, втемную. Примером такой акции, по всей видимости, является атака на кинокомпанию Sony Pictures, целью которой было предотвратить выпуск в широкий прокат комедийного фильма о главе КНДР.

Все больше интереса злоумышленники проявляют к мобильным платформам, прежде всего Android. По данным «Лаборатории Касперского», практически каждый пятый пользователь устройств на этой платформе в прошлом году сталкивался с вредоносным ПО. Количество зловредных программ для мобильных платформ измеряется уже сотнями тысяч и продолжает быстро расти. В 2014 году их число увеличилось более чем в 10 раз. При этом само ПО подверглось заметной эволюции. Если раньше типичный вирус проявлял активность в том, что рассылал СМС на платный номер, то теперь функциональность мобильных вирусов практически такая же, как и вирусов для настольных платформ. Счет троянцам, направленным на хищение финансовых средств, идет на многие тысячи. Вредоносное мобильное ПО активно используется и в целях шпионажа, ведь смартфоны и планшеты обладают средствами фиксации аудиовизуальной информации.

Относительно новым явлением последних месяцев стала активизация программ-вымогателей, которые зашифровывают файлы данных и требуют денег за их расшифровку. Они сменили «популярные» до того вирусы-блокировщики, для восстановления требовавшие отправить СМС на платный номер. К программам-вымогателям нового поколения можно отнести такие решения, как CryptoLocker, CryptoWall, TorLocker, CoinVault, TeslaCrypt и CTBLocker. У некоторых из них существуют версии, ориентированные на мобильные устройства.

Заражение происходит, как правило, через открытие зараженного вложения в электронное письмо или после посещения зараженной веб-страницы. После этого вирус в фоновом режиме шифрует файлы данных с помощью криптостойкого алгоритма и по окончании уведомляет об этом пользователя, требуя денег за расшифровку информации. По данным корпорации Dell, выручка злоумышленников, разработавших CryptoLocker, составила около 30 млн долларов за 100 дней.

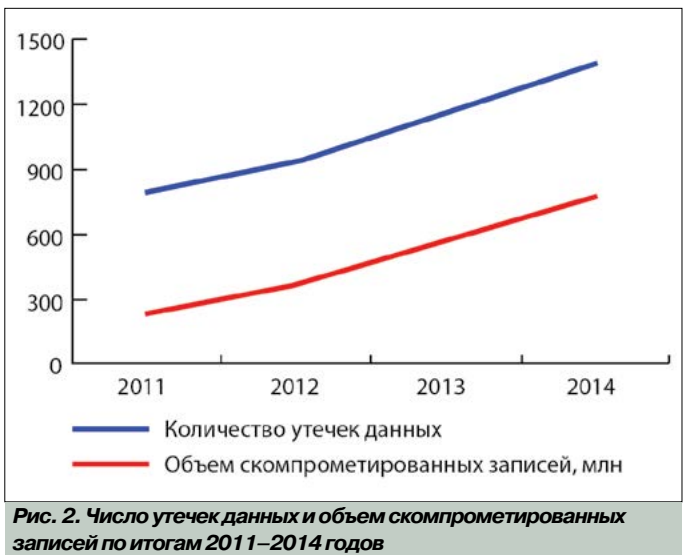


Рис. 2. Число утечек данных и объем скомпрометированных записей по итогам 2011–2014 годов

Особым случаем вредоносного ПО являются различные спам-программы. По итогам 2014 года, по данным «Лаборатории Касперского», доля спама составила немногим менее 67 % в общемировом объеме электронной почты. Однако в первом полугодии 2015-го, по информации Symantec, доля спама в мировом почтовом трафике опустилась ниже 50 %.

Связано это, по мнению экспертов, с мерами, которые принимались в течение последних пяти лет для борьбы с большими бот-сетями. В них участвовали и почтовые операторы, и интернет-провайдеры, и правоохранительные органы. По тем же самым причинам значительно снизились объемы спама в СМС и рассылках с использованием систем мгновенного обмена сообщениями. Не последнюю роль сыграло здесь совершенствование механизмов защиты от непрошеной почты. В итоге прибыльность рассылки спама для ее организаторов все это время неуклонно уменьшалась, что вынуждало их искать другие направления деятельности. Оказался затруднен и выход новых игроков на этот специфический рынок.

Спамеры пытались диверсифицировать свой бизнес, чтобы компенсировать потери от почтовых рассылок использованием других каналов. Это прежде всего касается социальных сетей и электронных медиа. Однако крупнейшие социальные сети пытаются бороться с этим явлением. Так, Twitter пошел по пути совершенствования технических способов противодействия, чтобы блокировать любые сообщения, нарушающие политику сети, в том числе рассылку рекламы. Facebook же решил прибегнуть к помощи правоохранительных органов, подав судебные иски против наиболее активных спамеров. Были попытки использовать в качестве канала для рассылки спама и мобильные приложения, которые распространялись с помощью манипулятивных технологий.

Положение дел с фишингом куда тревожнее. Особенно для российских пользователей, на которых, по оценке «Лаборатории Касперского», ориентирована каждая шестая фишинговая атака. С помощью таких технологий злоумышленники пытаются, и, к сожалению, чаще всего успешно, перехватывать аутентификационную информацию для различных интернет-сервисов, в том числе дистанционного банковского обслуживания, мобильного и интернет-банкинга. Тревожная ситуация наблюдается и с мобильными приложениями. По оценкам центра информационной безопасности одного из российских системных интеграторов, из 50 протестированных мобильных приложений российских банков только два были написаны с учетом всех требований к безопасности. Сейчас все, конечно, меняется к лучшему, но не очень быстро.

Однако, пожалуй, самый активный на сегодня сектор — утечки, связанные с персональными данными. Их количество продолжает расти. По сведениям компании InfoWatch, в 2014 году в мире произошло без малого 1400 утечек конфиденциальной информации, что на 22 % больше, чем годом ранее (рис. 2). Ущерб от них составил около 100 млрд долларов. При этом Россия, где отмечено 167 случаев, занимает второе место в мире по числу инцидентов. Соотношение умышленных и неумышленных инцидентов было практически равным, тогда как годом ранее доля умышленных утечек была несколько выше.

Если проанализировать информацию, полученную экспертами, то мы увидим, что большая часть утечек (92 %) относилась к персональным данным. На утечку коммерческих секретов и ноу-хау приходилось 4,2 %, государственных тайн — 1,7 %. Основными источниками утечек являются банки, розничная торговля, медицинские учреждения и интернет-сервисы. При этом почти 90 % скомпрометированных данных пришлось на мегаутечки, в ходе которых владельцы теряли 10 млн записей и более. Всего таких инцидентов было 14. В ходе еще 16 инцидентов был потерян миллион записей и более.

В России произошли две очень крупные утечки — кража идентификационных данных пользователей почты «Яндекс» и Mail.ru. В целом выводы аналитиков InfoWatch весьма тревожны: «Российская картина утечек стремительно приближается к американской. Многомиллионных утечек данных под воздействием внешних атак в России пока не зафиксировано. А вот мошенничество с чужими персональными данными в исполнении сотрудников банков, страховых компаний, салонов сотовой связи происходит чуть ли не ежедневно. Такие правонарушения стали нормой для нашей страны, хотя некоторое время назад казались экзотикой».

Самой дорогостоящей утечкой в России оказался инцидент в Санкт-Петербурге. Бывший сотрудник судоремонтного предприятия незаконно использовал технические документы десантного корабля «Зубр». Ущерб составил 3,5 млн рублей. В России в нынешнем году зафиксировано как минимум два случая очень крупных утечек, связанных с нарушением норм утилизации бумажных документов.

Главный редактор М. Сарбучев
Корректор Ю. Соболевская
Верстка О. Добренкова

Россия, 125047, Москва,
1-я Брестская ул., 35
Телефон: (499) 978-58-73,
(495) 251-76-50
Факс: (499) 978-57-36
E-mail: vestnik@kaskad.ru
http://www.kaskad.ru

Тираж 999 экз.

Распространяется по уникальной базе ПАО ЦНПО «КАСКАД»