PC WEEK RUSSIAN EDITION REVIEW
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ БИЗНЕСА
ИТ-БЕЗОПАСНОСТЬ
ФЕВРАЛЬ • 2013 • МОСКВА
http://www.pcweek.ru

ИТ-безопасность: итоги и тенденции 2012 г., перспективы 2013-го

ВАЛЕРИЙ ВАСИЛЬЕВ

Обратившись по традиции в начале нового года к экспертному сообществу, еженедельник PC Week/RE анализирует положение дел в области информационной безопасности (ИБ), сложившееся за прошедший год, и строит прогнозы на год предстоящий.

Кибероружие

Наиболее громкие заявления экспертов в области информационной безопасности прошедшего года относятся к констатации распространения и использования кибероружия в самых разных сферах жизни человеческого общества — в политике, экономике, науке, технике и т. д. От стандартных средств взлома кибероружие отличается сложностью разработки и применения, когда активно используются технологии целевых долговременных атак (Advanced Persistent Threat, APT), обеспечивающих скрытность проведения атаки на протяжении долгого времени — вплоть до нескольких лет. При этом эксперты заявляют о том, что создать кибероружие за два-три года по силам практически любой стране.

Высокую эффективность атак класса APT продемонстрировал взлом сертификатов программ компании Adobe, обнаруженный ею в конце сентября прошлого года. Этот взлом злоумышленники использовали для легитимации своих вредоносных программных разработок. Важно отметить, что сертификаты Adobe хранились с соблюдением правил обеспечения безопасности в специализированном аппаратном модуле, где среди прочих мер была задействована и криптозащита. И тем не менее сервер, выполнявший запросы на подпись программных кодов компании, был взломан.

Технология APT в данном примере открыла путь вредоносам в "белые списки" через взлом хранилища сертификатов, нарушив тем самым работу одного из эффективных и широко применяемых в настоящее время механизмов компьютерной защиты. Эксперты указывают и еще на один способ нарушения работы репутационных защитных механизмов — взлом непосредственно хранилищ "белых списков" с целью добавления в них регистрационных данных вредоносных программ.

Самая недавняя новость на тему применения кибероружия поступила в январе 2013 г. из "Лаборатории Касперского". Она касается проведённого ее специалистами исследования масштабной кибератаки, получившей название "Красный октябрь". Как информирует "Лаборатория Касперского", акция эта проводится злоумышленниками с 2007 г. с целью шпионажа в отношении дипломатических, правительственных и научных организаций, предприятий энергетики (в том числе ядерной) и космических агентств разных стран мира. Острие атаки направлено на страны Восточной Европы, Центральной Азии и бывшие республики СССР.

Кибероружие применяется не только для шпионажа, но и в диверсионных целях, в том числе с нанесением материального ущерба. Так, в августе прошлого года в ходе атаки Shamoon было выведено из строя более 30 тыс. компьютеров крупной нефтяной компании Saudi Aramco.

Характерно, что о виновниках применения кибероружия во время кибератак можно только догадываться исходя из того, кому эти атаки были выгодны. Эксперты отмечают, что располагать кибероружием и использовать его могут как государственные структуры (кибершпионаж, кибервойны), так и отдельные группы людей, которые руководствуются либо преступными мотивами (киберпреступность), либо стремлением к социальной справедливости (хактивизм).

Согласно прогнозам аналитиков корпорации Symantec, начиная с 2013 г. конфликты между государствами, организациями и даже отдельными лицами в значительной степени перейдут в киберпространство. При этом цель кибератак в основном будет состоять в том, чтобы причинить противнику ущерб или продемонстрировать свою силу, заявив таким способом о себе.

В прицеле злоумышленников — мобильные платформы

Эксперты отмечают лавинообразный рост числа вредоносных программ для мобильной платформы Android. По данным "Лаборатории Касперского", в 2012 г. их количество увеличилось примерно в шесть раз по сравнению с 2011-м и в пять раз превзошло суммарное число образцов вредоносных программ для Android, зарегистрированных Лабораторией с 2005-го по 2012 гг. Компания Trend Micro прогнозирует рост числа таких программ с 350 тыс. в 2012-м до 1 млн. в 2013-м.

Причина заключается в популярности и слабой защищенности этой платформы. Эксперты из "Лаборатории Касперского" рекомендуют специалистам, связанным с её развитием, воспользоваться опытом, накопленным за время жизни платформы Windows, чтобы не повторять уже выявленные стратегические ошибки развития операционных систем широкого использования в судьбе Android.

По мнению Марии Каншиной, менеджера по развитию бизнеса компании "Информзащита", недостатка в технических средствах защиты мобильных устройств на рынке сегодня нет. Однако разработчики пока не предлагают единого решения, которое позволяло бы обеспечить и централизованно управлять безопасностью сразу всех типов конечных точек пользовательского доступа. У г-жи Каншиной есть уверенность, что подобные продукты появятся на рынке в ближайшем будущем.

В 2012 г., отмечает генеральный директор компании "ДиалогНаука" Виктор Сердюк, возникла острая необходимость обеспечения удаленного доступа к корпоративным ИТ-ресурсам с мобильных устройств пользователей, включая мобильные телефоны и планшеты. Это привело к появлению на рынке специализированных продуктов по организации защиты такого доступа. Решения эти обеспечивают дополнительную аутентификацию пользователей, а также криптографически защищенное VPN-соединение, в том числе с возможностью применения отечественных средств шифрования. В нынешнем году г-н Сердюк прогнозирует увеличение спектра предлагаемых решений по организации удаленного доступа мобильных пользователей.

"Мобилизация" корпоративных пользователей стимулирует рост спроса на системы Mobile Device Management (MDM), который, как полагают наши эксперты, продолжится в наступившем году. Однако согласно оценке Владимира Овчарука, заместителя директора департамента внедрения и консалтинга компании LETA, MDM-системам пока еще не хватает полноты функциональности, а также удобства при эксплуатации и развертывании.

В условиях набирающего популярность движения BYOD ("принеси свое устройство в офис") важной функцией MDM-систем становится способность отделять пользовательские данные от корпоративных. Для этой цели, как отметил Владимир Удалов, руководитель направления корпоративных продуктов в странах развивающихся рынков компании "Лаборатория Касперского", используются "обернутые" (контейнеризированные) приложения. Суть такой технологии состоит в том, что приложение, обрабатывающее и сохраняющее корпоративные данные на мобильном устройстве, требует от пользователя дополнительной авторизации для доступа к этим данным. Кроме того, здесь применяется дополнительное шифрование данных контейнера, запрещается их копирование из контейнера вовне и передача в другие приложения.

Вместе с тем, по выражению Романа Кобцева, директора департамента развития и маркетинга компании "ЭЛВИС-ПЛЮС", тема BYOD остается для российских компаний "светлым послезавтра". Он считает, что ситуация в настоящее время такова: пока личные мобильные устройства сотрудников не наносят заметного урона корпоративной безопасности, на них просто не обращают внимания. Но как только урон превышает некий приемлемый для компании уровень, их тут же запрещают. Никакой интеграцией программы BYOD в общую архитектуру ИБ российские предприятия в массе своей пока заниматься не собираются.

Конец мифа безопасности Mac-платформы

Согласно данным "Лаборатории Касперского", в прошлом году троян Flashback заразил более 700 тыс. компьютеров Mac. По оценкам специалистов Лаборатории, ▸

Наши эксперты

МАРИЯ КАНШИНА, *менеджер по развитию бизнеса, "Информзащита"*

РОМАН КАРАСЬ, *начальник отдела маркетинга, CPS*

РОМАН КОБЦЕВ, *директор департамента развития и маркетинга, "ЭЛВИС-ПЛЮС"*

РОМАН КРЮЧКОВ, *технический директор, группа USN*

ЕВГЕНИЙ КУРТУКОВ, *руководитель отдела поддержки продаж, "Аксофт"*

ВЛАДИМИР МАМЫКИН, *директор по информационной безопасности, Microsoft в России*

Наши эксперты

ВЛАДИМИР ОВЧАРУК, *заместитель директора департамента внедрения и консалтинга, LETA*

АЛЕКСЕЙ САБАНОВ, *заместитель генерального директора, "Аладдин Р.Д."*

ВИКТОР СЕРДЮК, *генеральный директор, "ДиалогНаука"*

ВЛАДИМИР УДАЛОВ, *руководитель направления корпоративных продуктов в странах развивающихся рынков, "Лаборатория Касперского"*

МИХАИЛ ЧЕРНЫШЕВ, *технический консультант, McAfee в России и СНГ*

это самое крупное массовое заражение платформы MacOS X. Его причинами, по мнению экспертов, стали, с одной стороны, слепая вера многих поклонников Mac`ов в априорную безопасность своих компьютеров, а с другой — неоперативное исправление корпорацией Oracle уязвимостей в платформе Java (в результате, как свидетельствуют данные аналитических компаний, более половины регистрируемых ИБ-специалистами атак направлено на уязвимости Java и четверть — на уязвимости Adobe Reader). Очевидно, что пользователям MacOS не миновать того же пути, каким прошли пользователи Windows, у которых антивирусная защита установлена сегодня на более чем 90% компьютеров.

Тенденции в корпоративной защите

Результаты проведенного еженедельником PC Week/RE опроса позволяют ранжировать основные угрозы корпоративной безопасности так, как их видят не только специалисты ИБ-служб, но и обычные сотрудники, причастность которых к ИБ обусловлена их должностными обязанностями.

Преобладающим в российских компаниях фактором ИБ-риска является сегодня халатность в отношении политик ИБ со стороны рядовых сотрудников. Такую особенность российского персонала отметило более 80% респондентов. При этом на подобную же халатность со стороны разного уровня руководителей указывают в полтора раза меньше участников опроса. Вместе с тем о недостаточном внимании руководства к организации ИБ свидетельствовало почти 60% опрошенных.

О слабой организации информационной безопасности в российских компаниях говорит тот факт, что почти половина тех, кто принял участие в опросе, отметили неосведомленность рядовых сотрудников в отношении политик ИБ на своих рабочих местах. Увы, высока доля (35%) такой неосведомленности и в менеджерской среде.

В трети российских компаний остается актуальным злонамеренный инсайд со стороны рядовых сотрудников. А вот инсайд со стороны руководителей участники опроса считают явлением в три раза более редким. Взлома ИТ-систем злоумышленниками извне опасаются примерно в 24% российских компаний.

Несоответствие требованиям регуляторов, согласно результатам нашего опроса, корпоративные ИТ-пользователи относят к низким рискам — на них указывают 18% респондентов.

Консолидация корпоративных средств обеспечения ИБ, на которую эксперты обращают внимание на протяжении нескольких последних лет, по мнению Михаила Чернышева, технического консультанта McAfee в России и СНГ, продиктована не только (и не столько) желанием снизить операционные расходы на поддержку информационной безопасности, сколько стремлением через объединение всех модулей ИБ в единую экосистему реализовать проактивный режим защиты, без которого ИБ в современных условиях неэффективна, если не сказать невозможна.

Важной составляющей корпоративной системы безопасности становится анализ угроз. По словам г-на Чернышева, в мире уже немало реализовано проектов по централизации управления ИБ, охватывающих наряду с традиционными ИБ-средствами также и средства безопасности облачных сервисов.

Консолидация ИБ-ресурсов служит базой для перехода к централизованному управлению безопасностью, при этом, как отмечает Роман Кобцев, компании все чаще обсуждают варианты риск-ориентированных подходов, хотя до практического их ввода в действие дело пока доходит редко.

Роман Карась, начальник отдела маркетинга компании CPS, отмечает снижение рисков, связанных с отказами ИТ-инфраструктуры. Данный факт он объясняет постепенным переводом ИТ-ресурсов в ЦОДы высокой надежности, причем делают это не только крупные компании, но и представители среднего и малого бизнеса и даже владельцы домашних офисов. При этом приоритеты в обеспечении корпоративной ИБ смещаются в сторону защиты критических данных и повышения надежности информационных систем.

Для оперативного реагирования на ИБ-инциденты, согласно наблюдениям г-на Карася, крупные компании активно осваивают функционал центров управления инцидентами ИБ (Security Operation Center, SOC), а отдельные средние предприятия в целях централизации управления ИБ создают аналогичные по задачам группы специалистов или мини-SOC. В 2013 г. эта тенденция, как он полагает, закрепится, причем особое внимание в управлении информационной безопасностью компании будут уделять защите критически важных данных, улучшению политик безопасности, повышению культуры использования информационных систем.

Консолидация средств и централизация управления ИБ, как отмечает Виктор Сердюк, привела к существенному росту спроса в 2012 г. на решения класса управления информацией о безопасности и о событиях безопасности (Security Information and Event Management, SIEM). Внедрение таких решений позволяет существенно снять нагрузку с ИБ-администраторов и автоматизировать процессы управления инцидентами. Тенденции, связанные с ростом количества проектов по централизованному мониторингу событий ИБ, по его мнению, сохранятся и в 2013-м.

Подход большинства крупных вендоров к консолидации ИБ-средств и централизации управления ИБ, как заключает Владимир Удалов, состоит в том, чтобы расширять свою продуктовую линейку за счет поглощения небольших компаний, формируя в результате коммерческие комплексы, объединяющие несколько разных продуктов под одним зонтичным брендом. Этот подход, как он полагает, с одной стороны, позволяет быстро наращивать функционал таких комплексов, но с другой — чреват слабой интеграцией компонентов, которые могут работать несогласованно, не поддерживать единые сквозные политики и централизованное управление. Поэтому предпочтительным он считает комплексы моновендорные, т. е. от начала до конца созданные одним разработчиком.

Отмечая высокую безопасность ОС Windows 8, которая стала в области ИТ важной новостью прошлого года, эксперты из компании Trend Micro одновременно констатируют низкие темпы ее распространения в корпоративной среде. Они полагают, что в наступившем году доминирующей группой, которая сможет оценить преимущества улучшенных средств защиты новой ОС, окажутся домашние пользователи. По прогнозам аналитиков из Gartner, широкое корпоративное использование Windows 8 начнется не раньше 2014 г.

На фоне всеобщего признания актуальности угроз от инсайда (как злонамеренного, так и обусловленного неинформированностью или разгильдяйством пользователей) российский рынок DLP, согласно данным компании Anti-Malware.ru за 2012 г., вошел в фазу быстрого роста и в ближайшие пару лет будет расти на десятки процентов в год.

В то же время результаты опроса, проведенного еженедельником PC Week/RE, позволяют констатировать невысокую заинтересованность со стороны корпоративных заказчиков в юридической значимости результатов работы ИБ-систем, отличных от DLP. Хотя, казалось бы, при тенденции к консолидации данных, получаемых от корпоративных ИБ-систем, и к их централизованной обработке задачи так называемой апостериорной защиты от утечек чувствительной информации могли бы решаться и без развертывания DLP-систем. Факт отсутствия интереса к юридической значимости результатов работы ИБ-систем в среде российских корпоративных пользователей может быть связан с тем, что компании предпочитают предотвращать утечки, нежели бороться с ними через юридическое преследование тех, кто их допустил.

Обращаясь к теме юридической значимости функционирования корпоративных ИБ-систем, Алексей Сабанов, заместитель генерального директора компании "Аладдин Р.Д.", указывает на то, что в своей практике он такого понятия не встречал. Зато, отмечает он, есть широко распространенное понятие юридической силы электронного документа (ЮСЭД), есть принятое ИБ-сообществом понятие юридически значимого электронного документооборота. В 2012 г. вопросы ЮСЭД активно обсуждались на PKI-форумах в Киеве и Санкт-Петербурге, а также на парламентских слушаниях, прошедших 23 ноября 2012 г. в Совете Федерации РФ. Алексей Сабанов считает, что если все рекомендации, выработанные этими мероприятиями, утвержденные по итогам парламентских слушаний и направленные в адрес Федерального Собрания и Правительства России, будут выполнены, то в создании российского юридически значимого электронного документооборота произойдет реальный прорыв, по крайней мере с точки зрения его нормативно-правового обеспечения.

ИБ СПО

Евгений Куртуков, руководитель отдела поддержки продаж компании "Аксофт", отмечает, что несмотря на бурное развитие СПО, вопросы, связанные с обеспечением его информационной безопасности, затрагиваются редко. Он полагает, что связано это отчасти с бытующим в среде пользователей СПО мнением о том, что для Linux нет вирусов, отчасти с тем, что некоторые СПО-вендоры сертифицируют свои решения как средства защиты, формально закрывая этим требования госрегуляторов. По мнению г-на Куртукова, с появлением в России крупных СПО-проектов обеспечению информационной безопасности СПО будет уделяться больше внимания.

Как полагает Михаил Чернышев, в 2013 г. использование СПО в России, скорее всего, будет иметь лишь академический интерес, что, по его наблюдениям, происходило и в прошлом году. Он считает, что свободно распространяемые программные решения не конкурентоспособны по критериям ИБ в сравнении с решениями корпоративного класса. Рост спроса на СПО-решения если и будет зафиксирован, то лишь в сегменте среднего и малого бизнеса. Сегмент крупных компаний, на его взгляд, перенасыщен разрозненными неинтегрированными ИБ-решениями. Практического применения, заключает он, свободно распространяемое ПО для защиты информации традиционно не находит в силу возросших требований к безопасности.

Облака. Веришь — не веришь?

Корпоративное использование облачных сервисов тормозит недостаточная правовая проработка сферы отношений между провайдерами и потребителями облачных услуг и порождаемая этим проблема недоверия между ними. Компании (те, которым это по средствам) предпочитают строить свои частные облака. Все прочие (средний и малый бизнес, индивидуальные пользователи) погружаются в облачные сервисы на свой страх и риск, не имея достаточных юридических гарантий разрешения возможных конфликтных ситуаций.

Основной нерешенной проблемой безопасности облачных сред Алексей Сабанов считает отсутствие метрик и инструментов измерения ИБ для облаков (и тем более

ПРОДОЛЖЕНИЕ НА С. 19 ▶

Безопасность клиентского удаленного доступа

ЕЛИЗАВЕТА СПАСЕННЫХ, МЕНЕДЖЕР ПО РАЗВИТИЮ БИЗНЕСА КОМПАНИИ "ИНФОРМЗАЩИТА"

Вопросы обеспечения безопасности клиентского удаленного доступа в последнее время не теряют своей актальности. На тему удаленного доступа регулярно публикуют свои отчеты аналитические компании (в том числе IDC и Gartner). Средства защиты удаленного доступа клиентов к ресурсам совершенствуются буквально с каждым днем. Объектом защиты в первую очередь является информация, к которой клиенты получают доступ в рамках дистанционного получения услуг (платежная информация, персональные данные, коммерческая тайна или иная информация ограниченного доступа и т. д.). К таким услугам чаще всего относят государственные сервисы, дистанционное банковское обслуживание или интернет-банкинг, электронную коммерцию.

Обеспечение безопасного удаленного доступа обычно требует реализации надежных механизмов идентификации и аутентификации пользователей, шифрования передаваемого трафика и разграничения доступа внутри ресурса, к которому осуществляется доступ. Состав средств безопасности при этом определяется тремя ключевыми факторами:

- результаты анализа угроз, учитывающего особенности информации, к которой предоставляется доступ;
- требования регуляторов к защите информации (например, Федеральный закон № 152 "О персональных данных", Федеральный закон № 161 "О национальной платежной системе" и соответствующие подзаконные акты);
- необходимый уровень обеспечения доступности информации.

Однако обеспечение безопасного удаленного доступа требует не только использования технических мер защиты, но и ряда организационных мероприятий. Их целью является повышение осведомленности лиц, которые получают удаленный доступ. Эти меры приобретают особенную актуальность в свете все более широкого распространения методов социальной инженерии, с использованием которых мошенники могут воздействовать на субъектов удаленного доступа и обходить любые технические меры защиты.

При выборе средств защиты удаленного доступа важно вначале определить, к какому из трех типов клиентов доступ предоставляется. Работникам ли компании, лицам ли, получающим услуги на основании договора или же без заключения такового.

В первом случае сервис предоставляется в рамках внутренних процессов компании ее сотрудникам. Благодаря чему у компании есть возможность управлять процессами ИБ на всех уровнях (контроль за своевременным изменением учетной информации, использование антивирусных средств, обеспечение работы механизмов доверенной загрузки и прочее).

Во втором — невозможность контроля среды работы пользователя приводит к повышению рисков несанкционированного доступа к защищаемой информации (например, с использованием вредоносного ПО). Однако компания имеет возможность контролировать процессы передачи индентификационной и аутентификационной информации пользователям.

Наконец, для третьего типа клиентов (то есть в случае, когда услуга предоставляется в массовом масштабе) возможность использовать надежные средства аутентификации становится минимальной. Часто парольная информация направляется по открытым каналам (по электронной почте). А "доверенность" среды работы пользователя зависит лишь от него самого.

Соответственно наиболее "проблемными" являются вторая и третья категория пользователей. Проблемы и тенденции по обеспечению их безопасного удаленного доступа рассматриваются ниже.

В 2012 г. вступило в силу Постановление правительства № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". В соответствии с ним для всех используемых средств защиты, закрывающих актуальные угрозы, должна быть проведена процедура оценки соответствия требованиям законодательства РФ. Также для случаев, когда угроза использования недокументированных (недекларированных) возможностей (НДВ) признана актуальной, данное Постановление определило необходимость проведения контроля наличия НДВ для всего системного и (или) прикладного программного обеспечения, используемого в информационной системе.

Эти требования распространяются и на средства, используемые для построения систем безопасного удаленного доступа. Вероятно, производители таких средств теперь будут вынуждены проверять свои решения на отсутствие НДВ, так как актуальность угрозы их использования определяется на этапе формирования модели угроз для конкретной системы. Требования к использованию сертифицированных средств защиты предъявлялись и прежде. Однако если раньше они распространялись на ограниченное число систем и организаций, то сейчас данное требование обязательно для выполнения во всех коммерческих и государственных информационных системах персональных данных. Для обычных пользователей это означает необходимость проведения дополнительных действий для получения доверенных учетных данных. Для компаний, предоставляющих услуги или сервисы в государственном масштабе, — повышение затрат на обеспечение безопасности.

Также в 2012 г. вступила в силу значительная часть положений Федерального закона № 161 "О национальной платежной системе". В результате на операторов платежных систем была возложена ответственность за возврат денежных средств клиенту в случае их несанкционированного списания. Таким образом, может сложиться ситуация, что банки, не имея возможности исключить негативное влияние сторонних факторов на пользователей (например, вредоносных программ на рабочих местах пользователей, осуществляющих несанкционированный перехват и передачу данных), должны обеспечить защиту их рабочих мест в целях минимизации собственных рисков. Такое положение дел незамедлительно привело к существенному увеличению уровня мошенничеств в банковской сфере. Атакам все чаще подвергаются не периметровые средства защиты, а контактные центры обслуживания абонентов и сами клиенты.

В целях исключения негативного влияния внешних факторов операторы платежных систем начали работу по совместному выявлению новых методов мошенничества и формированию интеллектуальных методов противодействия им (таких, как система фрод-мониторинга). Вместе с тем банки все чаще используют усиленные средства аутентификации и специализированные устройства, обеспечивающие доверенную среду для заверения документов, формируемых в рамках сеансов удаленного клиентского доступа.

Разработка и внедрение организационных и технических мер, направленных на выявление новых способов мошенничества, противодействие атакам на традиционные средства защиты и активным методам социальной инженерии, станут одним из главных трендов 2013 г.

СПЕЦПРОЕКТ КОМПАНИИ "ИНФОРМЗАЩИТА"

In или Out – какой Source выбрать?

СЕРГЕЙ ПАНОВ, ДИРЕКТОР ТЕХНИЧЕСКОГО ДЕПАРТАМЕНТА ОАО "ЭЛВИС-ПЛЮС"

— Не люблю интеграторов.
— Ты просто не умеешь их готовить!

В последние месяцы в различных СМИ и на интернет-площадках участились дискуссии по вопросу "Делать самим или привлечь интегратора?". Зачастую особый накал таких "бесед" вызван не реальным положением вещей, а недопониманием того, чем занимаются системные интеграторы (СИ), и недостатком диалога "интегратор — аудитория". Хотелось бы восполнить этот пробел и рассказать, как всё происходит на самом деле.

В первую очередь следует помнить, что есть два направления системной интеграции (иногда они пересекаются, но далеко не всегда) — это ИТ-интеграция и интеграция в области информационной безопасности. Второй рынок значительно меньше по объёмам и по количеству участников (доказательство тому — аналитические обзоры и рейтинги), поэтому правила игры здесь сильно различаются. "ЭЛВИС-ПЛЮС" работает на рынке ИБ-интеграции, поэтому речь пойдёт именно о нём.

Основные темы, которые вызывают наибольший ажиотаж, такие: необоснованно высокая стоимость проектов (или, попросту говоря, жадность), несоответствие результата практическим и реальным требованиям заказчика и значительное время реакции на нештатные ситуации.

Сначала поговорим о деньгах. Главное правило тут таково: проект стоит столько, сколько он стоит, и не больше, чем заказчик готов за него заплатить. "ЭЛВИС-ПЛЮС" уделяет особое внимание обоснованию стоимости работ и услуг в коммерческом предложении или заявке на конкурс. Существует и другой подход к формированию стоимости предложения системным интегратором — ориентация на сверхприбыль (и надо признать, что такой подход тоже имеет право на существование, мы не можем здесь никого осуждать). Такие интеграторы выставляют заведомо завышенную стоимость проекта, надеясь на "авось получится". И иногда действительно получается. Наша же компания проповедует диаметрально противоположную философию: мы ориентируемся на длительное сотрудничество с партнёром и на поддержание своей репутации. А на нашем рынке репутация крайне важна, ведь рынок в общем-то камерный, все про всех знают и могут оценить предложения конкурентов с некоторой достоверностью.

Второй распространённой темой является несоответствие результата ожиданиям заказчика. Почему-то считается, что заплатив деньги интегратору и дистанцировавшись от проекта, заказчик должен получить идеальный результат. При этом зачастую изначально заказчик не может даже сам для себя сформулировать, как именно должен выглядеть пресловутый идеальный результат. Но ведь проект с интегратором — тоже управленческая задача! И интегратор — это хорошо подготовленный, опытный и высококвалифицированный ресурс, который необходимо уметь правильно использовать!

Почему-то считается, что заплатив деньги интегратору и дистанцировавшись от проекта, заказчик должен получить идеальный результат.

Заказчик обязательно должен совместно с интегратором сформулировать постановку задачи; совместно с ним спланировать общие действия, которые позволят эту задачу решить; отследить и проконтролировать результаты. В противном случае подрядчик либо реализует своё видение решения проблем заказчика, либо поставит типовое решение, которое ему наиболее удобно и наименее для него затратно. И это будет управленческой ошибкой заказчика, которая проявится в том числе и в неправильном выборе интегратора.

Часто приходится слышать о том, что интегратор слишком долго реагирует на изменение ситуации. Под этим может подразумеваться и не слишком быстрая реакция на ЧП (выход из строя оборудования или ПО, целенаправленная атака и т. п.), и недостаточно оперативное совершенствование системы защиты информации заказчика. Есть несколько путей решения этой проблемы: заключи с интегратором (или аутсорсером) SLA (наказывать деньгами за неисполнение обязательств); информируй интегратора о свои проблемах; сделай его своим партнёром и держи его в курсе своих ИБ-планов — тогда тебе смогут предложить современное решение.

Привлекая к работам и проектам аутсорсеров, заказчик преследует несколько целей. И если рынок системной интеграции есть и растёт из года в год, то должны быть и преимущества, которые получает заказчик от такого сотрудничества. Глобально все эти преимущества можно выделить в пять больших групп (в порядке убывания важности для заказчика, по моему мнению): квалификация и экспертиза, управление проектной деятельностью, конкуренция, финансовая выгода и разделение ответственности.

Безусловно, самым значимым бонусом, который получает заказчик от сотрудничества с СИ, является предоставляемая интегратором экспертиза. Можно со всей ответственностью утверждать, что опыт сотрудников, ежедневно вовлечённых в решение самых сложных, крупных и разнообразных задач (а именно такой является работа в штате СИ, и многие специалисты сознательно выбирают для себя этот нелёгкий, но увлекательный путь), будет значительным. И дело даже не в решении повседневных задач заказчика (с ними отлично справляются и его сотрудники) — дело в более широком видении проблем. Специалисты интегратора знают и отслеживают риски и могут предложить пути компенсации и минимизации этих рисков в будущем. Как защититься от специфических для отрасли видов угроз? Как снизить возможные потери? Как выполнить требования нормативно-правовых актов и пройти проверки регуляторов? Невозможно ответить на эти вопросы, не столкнувшись с ними несколько раз. У крупных интеграторов в портфолио десятки успешных проектов, а у "ЭЛВИС-ПЛЮС", например, они ещё и в различных отраслях.

Результат внутренних проектов заказчика во многом определяется эффективностью управления проектной деятельностью и наличием компетентной проектной команды. О команде мы поговорили в предыдущем пункте, но нельзя отрицать и важность проектного менеджера, человека, который будет управлять ресурсами, временем и взаимоотношениями между всеми людьми, вовлечёнными в реализацию проекта. Готовы ли собственные менеджеры к решению таких задач? Интегратор предоставляет не только такого человека, но и технологии управления. Это хороший способ достижения поставленных целей.

Безусловно, самым значимым бонусом, который получает заказчик от сотрудничества с системным интегратором, является предоставляемая им экспертиза.

Для заказчика большим преимуществом является то, что уровень конкуренции на рынке ИБ достаточно высок. Сейчас это рынок заказчика. И очень мало кто из системных интеграторов может диктовать свои условия. Это стимулирует интеграторов выдавать реальные, хорошо просчитанные и обоснованные предложения. Можно собрать нескольких потенциальных подрядчиков, столкнуть их лбами и получить более выгодное по содержанию предложение. Сработает ли аналогичный подход с собственной службой — большой вопрос.

Финансовая выгода. С одной стороны — это самое очевидное преимущество, с другой — и самое неоднозначное. Дело в том, что один и тот же проект (по составу работ и оборудования) в одной ситуации может оказаться дороже, если привлечь интегратора, а в другой — если выполнять силами самого заказчика. Одинаковых проектов почти не бывает, и каждый надо просчитывать заново. Часто заказать проект у интегратора получается дешевле, чем делать его своими силами. Разница в цене особенно заметна в случае кратко- и среднесрочных проектов с привлечением дорогостоящих специалистов. Если заказчик считает, что внедрение решений, предложенных интегратором, слишком дорого, ему имеет смысл рассчитать стоимость внутреннего проекта, используя такой же подход, который используем мы для выставления коммерческих предложений. Иногда результат может сильно удивить.

И неочевидное (только поэтому оно стоит последним), но не менее важное и значимое преимущество — разделение ответственности с интегратором. Сюда входят компетентный взгляд на проблемы заказчика со стороны; заключение соглашений об уровне обслуживания; договорные обязательства интегратора, связанные с работоспособностью тех или иных систем. Ведь главное, за что платят интегратору, — не поставка оборудования и привлечение специфических и квалифицированных специалистов, а решения проблем заказчика, которые продумывает интегратор и за которые он берёт ответственность (назовём это "думать за заказчика"). А также "головная боль", связанная с внедрением этих решений. И не следует забывать один немаловажный нюанс: интегратор отвечает перед заказчиком в соответствии с договорными обязательствами, а собственные сотрудники заказчика — в соответствии со своими должностными обязанностями, которые далеко не всегда вдохновляют на исполнение специфических интеграторских задач, требующих определенного навыка, творческого подхода и в конце концов выделенного рабочего времени!

Подводя итог, повторюсь: каждый проект уникален. И в каждом проекте нужно считать деньги и время. Иногда выгоднее (по самым разным параметрам) заказать разработку и осуществление проекта интегратору. Иногда — делать самим. Иногда — сделать выбор в пользу комплексного решения. Главное — рассмотреть ВСЕ возможности, не следовать за собственным настроением и настроением окружающих. А самым ярым критикам СИ хочу дать один совет: не считайте чужие деньги. В крупных проектах заказчик уже посчитал их и принял самое выгодное для себя решение.

Как уже было отмечено, зачастую сторонам не хватает обратной связи. Если у вас есть что сказать нам, пишите в Твиттер — twitter.com/ELVIS_PLUS.

ИТ-безопасность...

◀ ПРОДОЛЖЕНИЕ СО С. 17

стандартов), и пока у сообщества экспертов нет на этот счет каких-либо конструктивных предложений. Он полагает, что ситуация здесь будет улучшаться по мере накопления практического опыта работы в облаках различных типов. В то же время с 2013-м больших ожиданий по этой части он не связывает.

В наступившем году, по мнению г-на Сабанова, должны быть получены ответы на вопросы юридической ответственности между провайдерами и потребителями облачных сервисов, а также в обществе должно быть достигнуто понимание того, что необходимо строить пространство доверенных сервисов (по определению Алексея Сабанова — единого пространства доверия) в облаках, особенно публичных, что во многом он связывает с планируемым переносом некоторых функций государственного управления в облачную среду.

Эксперты отмечают, что для защиты виртуальных и облачных сред уже используются антивирусы, системы обнаружения вторжений и межсетевого экранирования, системы контроля доступа к виртуальной инфраструктуре, средства ее защиты на протяжении полного жизненного цикла — от момента подготовки и инициализации до уничтожения. Вместе с этим г-н Куртуков обращает внимание на явное доминирование в ассортименте этих продуктов таких, которые ориентированы на платформу VMware, и отмечает недостаток поддержки других платформ виртуализации.

Что касается оценки эффективности существующих продуктов, предназначенных для обеспечения ИБ облачной ИТ-инфраструктуры, то компания Trend Micro, один из лидирующих поставщиков комплексных средств защиты облаков, в конце 2012 г. по этому поводу высказалась неожиданно пессимистично: ее специалисты считают, что имеющиеся ныне средства безопасности все-таки не способны защитить данные в облачных инфраструктурах.

Как отмечает Владимир Овчарук, в настоящее время нет единой точки входа в облачные сервисы, предоставляемые разными провайдерами, и в случае полного или частичного вывода бизнес-процессов в облака организация-клиент вынуждена передавать свои данные сразу в несколько внешних компаний, что, по его мнению, может быть просто неприемлемым для бизнеса. Кроме того, в этой ситуации для клиента теряется прозрачность инфраструктуры и контроль над ней, становятся высокими риски нарушения целостности и конфиденциальности информации, обрабатываемой в облаке, а также риски, связанные с доступностью выведенных в облако сервисов.

К наиболее критичным задачам, которые возникают в связи с обеспечением ИБ облачных сервисов, Мария Каншина относит идентификацию и аутентификацию клиентов. При этом главные проблемы она тоже видит в юридических и организационных аспектах, которые касаются распределения ответственности в виртуальных средах между участниками процесса предоставления облачных услуг.

Обеспечение ИБ в облачных условиях, как подчеркивает г-н Мамыкин, директор по информационной безопасности Microsoft в России, требует изменения бизнес-процессов внутри отделов ИБ у клиентов облачных сервисов, что, согласно его наблюдениям, недостаточно осознается ими. При работе с облачными сервисами специалистам компании-клиента надо

ПРОДОЛЖЕНИЕ НА С. 20 ▶

СПЕЦПРОЕКТ КОМПАНИИ MCAFEE

McAfee Network Security Platform

АНДРЕЙ НОВИКОВ, МЕНЕДЖЕР ПО РАБОТЕ С КЛЮЧЕВЫМИ ЗАКАЗЧИКАМИ

Данная статья посвящена не просто очередному продукту очередного вендора. Речь в ней пойдёт о новом подходе к обеспечению безопасности, центром которого является McAfee Network Security Platform. В последние годы мы все чаще и чаще сталкиваемся с совершенно новыми, очень сложными атаками на наши корпоративные ресурсы. Виной тому в том числе стало объединение хакеров в весьма серьёзные организации. Отличным примером здесь может служить группа Anonymous. Эти парни терроризируют мир, и почти каждая их атака становится глобальной проблемой для атакуемой организации. Взламываются сети государственных учреждений и заводов, ставится под угрозу национальная безопасность целых государств. Пора бы объединить и безопасность в вашей сети!

Реактивный подход к обеспечению безопасности не приносит желаемого результата — сегодня невозможно решить проблему, пытаясь обнаружить источники угроз и запретить доступ к ним. Постоянное тотальное блокирование источников заражения приведёт к тому, что довольно часто вам придётся блокировать доступ ко вполне легитимным ресурсам, а это плохую службу сослужит бизнесу вашей компании. Устранение последствий любого серьёзного инцидента в области безопасности должно начинаться с определения корня возникновения проблемы, приведшей к инциденту. В разобщенных системах безопасности сделать это нельзя, так как вы не знаете и не видите всю картину происходящего в ваших сетях. Пришло время отказаться от медленных, старых, не готовых к интеграции с другими элементами безопасности систем обнаружения вторжений. Они должны быть отправлены на заслуженный отдых. Мы в McAfee (100%-ная дочерняя компания Intel) предлагаем решить проблему безопасности с помощью принципиально нового подхода. Наша основная философия — объединение всех модулей безопасности в единую экосистему. Без такого объединения невозможно говорить о полноценной защите корпоративных ресурсов. McAfee Network Security Platform является ключевым продуктом, позволяющим объединить разрозненные системы безопасности в единую экосистему. В конце концов, представьте себе торговую организацию, в которой работает 100 или 200 сотрудников, и эти сотрудники никогда не общаются между собой, никто никому не ставит никаких задач, никто ни с кем не советуется при принятии тех или иных решений. Будет ли такая организация работать эффективно? То же самое происходит и с безопасностью. Одиночки не справляются. Нет и никогда не будет идеальных систем, способных решить любую проблему. Если отдельные задействованные в системе безопасности решения не будут обмениваться информацией об угрозах любой активности пользователей, баз данных, почтовых и веб-серверов, биллинговой системы и используемых в сети приложений, то невозможно построить действительно эффективную систему безопасности!

На рынке существует огромное множество решений, и все только и говорят о том, сколько новых галочек и функций появилось в новой версии того или иного продукта, какая достигнута производительность и т. д.! При этом никто не говорит, как объединить все те 10 или 20 решений по безопасности во что-то единое, быстрое, интеллектуальное, способное предугадывать ситуацию и готовое к отражению самых изощрённых атак.

Новая версия IPS/IDS-решения McAfee Network Security Platform, с 2003 г. находящаяся в группе лидеров в магическом квадранте Gartner, имеет обширную базу сигнатур для самых разных атак, в том числе на SCADA-системы. Это решение позволяет визуализировать весь трафик в корпоративной сети вплоть до приложения, имени пользователя, источника риска. Оно способно защитить ваши ресурсы от DOS/DDOS-атак, от нападок со стороны бот-сетей, от вирусов, пытающихся проникнуть в вашу инфраструктуру. При этом благодаря интеграции с vCenter компании VMWare оно обеспечивает защиту как физических, так и виртуальных устройств. Подтвержденная производительность McAfee Network Security Platform составляет до 10 Гбит/с на одно устройство со всеми включёнными правилами (в том числе при включении проверки SSL).

Но все это не главное. Главное то, что McAfee Network Security Platform может выступить в роли центра для принятия решений по инцидентам в системе безопасности. В данном случае под IPS мы понимаем целую платформу, а не просто отдельный продукт.

Самое важное сегодня — это поддержка внешних контекстов. Речь идёт не просто о способности продукта интегрироваться в сторонние консоли для выдачи оповещений об инцидентах в системе безопасности, а о полноценном его встраивании в другие решения, благодаря чему можно построить полноценную платформу, состоящую из кросс-функциональных продуктов.

McAfee Network Security Platform нативно поддерживает технологию GTI, позволяющую определять репутацию файла, сети, домена, IP-адреса, URL, уязвимости. GTI является самой крупной базой репутаций в мире. Поддержка данной технологии также позволяет McAfee IPS динамически изменять действия, применяемые к коммуникации с определённым ресурсом. Например, McAfee IPS может блокировать соединения с ресурсами, имеющими плохую репутацию, и отправлять в карантин соединения с ресурсами, имеющими среднюю репутацию. При этом изменение рейтинга ресурса в базе GTI приведёт к автоматическому изменению действия со стороны McAfee IPS. Среди прочего GTI помогает в выявлении неизвестных атак. Исследовательский центр McAfee Labs изучает известные и возможные неизвестные угрозы, результатом чего становится наличие в базе GTI уникальной всеобъемлющей информации по безопасности (так называемая безопасность на 360 градусов). Данная технология оправдывает своё использование на протяжении многих лет. Отличным примером служит то, что GTI в своё время помогла нашим клиентам защититься от таких атак, как “Аврора”, “Стакснет”, “Красный Октябрь” и другие. Вы наверняка каждый день читаете о новых и новых клонах самых разных угроз, начиная с вирусов и заканчивая эксплойтами. GTI знает о самом главном! GTI изучает векторы атаки, GTI знает, как выглядит основа атаки, GTI знает о сущности атаки, GTI знает, как защитить вашу инфраструктуру даже без обновления каких-либо сигнатур.

McAfee Network Security Platform поддерживает нативную интеграцию с анализатором уязвимостей McAfee Vulnerability Manager, что позволяет динамически изменять правила защиты для определённых активов. Например, McAfee IPS может самостоятельно определить, какие правила защиты будут работать для хостов на базе Windows, а какие будут работать для серверов под управлением Linux. При этом изменение версии или типа ОС на хосте приведёт к автоматическому изменению правила, применяемого для данного хоста. К тому же вы можете осуществлять сканирование любых хостов на наличие у них уязвимостей, не покидая консоли управления IPS.

McAfee Network Security Platform поддерживает нативную интеграцию с McAfee Host IPS, позволяющей продуктам делиться информацией об угрозах, зафиксированных на уровне сети и уровне хоста. При этом McAfee IPS может динамически влиять на правила защиты, применяемые на Host IPS.

McAfee Network Security Platform поддерживает интеграцию с McAfee SIEM. Обладая широкими возможностями по объединению всех источников событий корпоративной сети, будь то коммутатор, маршрутизатор, база данных или кассовый аппарат, McAfee SIEM позволяет McAfee Network Security Platform получить всеобъемлющую картину происходящего в сети, тем самым предоставляя возможность влиять на правила защиты для любого участника вашей инфраструктуры в автоматическом режиме.

Давайте вспомним время, когда в наших компаниях не было ERP-систем. Управление трудовыми ресурсами существовало отдельно, управление финансами — отдельно, управление активами — отдельно. В какой-то момент все поняли, что без объединения всех элементов управления предприятием в единую систему не будет развития, не будет возможности опередить соперника в конкурентной борьбе. То же самое происходит сегодня на рынке безопасности. Превратите свою инфраструктуру безопасности в удобную экосистему, в которой для решения самых сложных вопросов, для защиты вашего бизнеса потребуются секунды, а не часы, а то и дни.

Компания McAfee выводит на рынок новую объединяющую платформу, способную противостоять самым сложным атакам. В текущем году платформа McAfee Network Security Platform получит сертификат ФСТЭК по 5-му уровню защиты.

ИТ-безопасность...

◀ ПРОДОЛЖЕНИЕ СО С. 19

решать совершенно новые задачи, нежели в традиционной архитектуре ИТ. Им придется обеспечивать ИБ, тесно взаимодействуя с персоналом провайдера облачных сервисов. Это требует от клиентов умения работать с “железом” и софтом не только непосредственно на своей территории, но и на территории провайдера, и зачастую не своими руками, а через его специалистов. В таких условиях на первый план выходит умение составлять договора на обслуживание и контролировать их исполнение, определять ключевые метрики ИБ, применяемые к облачным услугам, и отслеживать их выполнение, оценивать риски третьих сторон, обучать и самим быть обучаемыми. Владимир Мамыкин обращает внимание на то, что это задачи в гораздо большей степени управленческие, нежели технические.

По мнению Романа Крючкова, технического директора группы USN, в 2012 г. рынок не увидел принципиально новых решений в сфере защиты облачных данных. В результате наиболее важную для себя информацию компании все еще предпочитают хранить на внутренних ИТ-ресурсах. С технологической точки зрения, как полагает г-н Крючков, обеспечить требуемую клиентами надежность защищенности данных в облаке вполне возможно. Однако стоимость таких решений окажется неприемлемо высокой для корпоративного рынка. Тем не менее несмотря на это, как он отмечает, количество корпоративных пользователей облачных сервисов увеличивается, хотя и невысокими темпами.

В настоящее время, по наблюдениям г-на Удалова, компании, размещая свою информацию в публичном облачном сервисе, не имеют возможности контролировать уровень обеспечения ее безопасности. Причины этого он видит в том, что провайдеры облачных сервисов не допускают клиентов к проведению аудита защищенности своих серверов, и даже если это не так, то далеко не у каждого клиента найдутся специалисты с необходимой для проведения аудита квалификацией. Владимир Удалов предполагает, что в ближайшем будущем появятся компании-посредники, которые будут специализироваться на независимых проверках состояния информационной безопасности публичных облачных сервисов, наряду с институтом сертификации для определения уровня безопасности проверяемых сервисов.

Самим же компаниям, пользующимся облачными сервисами провайдеров, г-н Удалов советует в первую очередь обращать внимание на безопасность конечных устройств — рабочих станций и серверов. Если они оказываются недостаточно защищены, то злоумышленники через них могут получить доступ ко всем данным, хранящимся в облаке.

Согласно данным корпорации Symantec, 77% компаний испытывают сложности из-за самовольного использования персоналом облачных решений в обход корпоративных правил. Поэтому, как подчеркивают наши эксперты, важно не только декларировать внутренние ИБ-политики, регламентирующие в том числе и доступ к облакам, но и наладить контроль их исполнения наряду с механизмом привлечения к ответственности за нарушения.

Особая актуальность таких мер связана со взломами пользовательских данных в социальных сетях, облачных сервисах, на серверах многопользовательских онлайновых игр, которые демонстрируют, что при ▶

использовании облачных технологий, когда миллионы учетных записей хранятся на одном сервере, а доступ в Интернет осуществляется по высокоскоростным каналам, угроза утечки информации обретает колоссальный масштаб.

Госрегулирование: пере- и недо-

Как считает Евгений Куртуков, государственное регулирование аспектов ИБ имеет для нашей страны особенное значение, поскольку многие российские организации и предприятия при формировании корпоративных ИБ-политик ориентируются исключительно на формальное соблюдение требований законодательства, а не на реальные потребности бизнеса.

Сходное мнение о ситуации на национальном рынке ИБ у Романа Кобцева. По его оценкам, до 80% всех проектов внедрения решений ИБ в нашей стране обусловлены сегодня (и в ближайшем будущем тоже) выполнением требований к защите информации со стороны регуляторов. Он обращает внимание на то, что с позиции оценки ИБ-угроз и связанных с ними рисков это неправильно. Однако на сложившуюся ситуацию он рекомендует посмотреть с позиции бизнес-рисков. Тогда становится очевидным, что одним из главных рисков практически для любой работающей в России компании в настоящее время является несоответствие требованиям законодательства.

Ссылаясь на данные исследований компаний Ernst&Young и Oxford Analytica, г-н Кобцев сообщает, что риски, связанные с информационной безопасностью, входят в первую десятку бизнес-рисков только в двух отраслях — в банковской и в разработке новых технологий. Поэтому к основным драйверам российского ИБ-рынка на протяжении ближайших лет г-н Кобцев относит требования регуляторов к обеспечению безопасности государственных информационных ресурсов, к защите персональных данных, к безопасности национальной платежной системы и межведомственного электронного взаимодействия.

Роман Кобцев уверен, что этот рынок по-прежнему в основном будет ориентирован на государственный и крупный корпоративный сектора, а в сегменте СМБ продаж средств защиты будет гораздо меньше. Важные изменения, по его прогнозам, должны произойти в национальном оборонно-промышленном комплексе, где на смену пока преобладающим физическим средствам защиты идут современные ИБ-технологии. Конкурентоспособность на международной арене в области разработки вооружений требует активного внедрения новых технологий для проектирования и производства сложных изделий. Это, по его мнению, порождает как минимум две проблемы: требующие активного использования ЦОДов огромные объемы данных, обрабатываемых современными САПР, и необходимость поддержки совместной работы над проектами нескольких предприятий, что нуждается в активном сетевом взаимодействии.

Заметно усилилось внимание государства к ИБ критических инфраструктур. Однако, обращаясь к опыту США, г-н Кобцев не ожидает в этом году появления сформированной нормативно-правовой базы, на основе которой можно было бы запустить государственные надзорно-контрольные функции на полную мощность, — слишком много остается проблем, как технических, так и правовых, а без четких правил игры, по его мнению, внедрение решений, необходимых для защиты критических инфраструктур, останется уделом узкого сегмента компаний-новаторов из числа крупных предприятий ТЭК, которые могут себе позволить долговременные проекты.

Прошедший год знаменателен сразу несколькими инициативами регуляторов в области ИБ. Так, Госдума РФ в июле 2011-го приняла поправки, внесенные в закон "О персональных данных", относящиеся к его применению, понятиям и принципам обработки персональных данных. Однако результативность всех поправок и изменений, внесенных в этот закон за семь лет его существования, у операторов персональных данных вызывает сомнения.

Алексей Сабанов обращает внимание на то, что вышедшее 1 ноября 2012 г. постановление правительства № 1119 наряду с ожидаемыми разъяснениями положений закона "О персональных данных" неожиданно для многих специалистов породило ряд новых вопросов, особенно по поводу угроз, связанных с недокументированными (недекларированными) возможностями, требования к которым традиционно учитывались при обеспечении конфиденциальности, целостности и доступности защищаемой информации. У г-на Сабанова вызывает большие сомнения, что усугубление и без того излишней зарегулированности в области обращения персональных данных приведет к реальному повышению их защищенности.

Далеко не полностью, по мнению экспертов, прояснил ситуацию с регулированием применения электронной подписи в стране принятый весной 2011-го закон "Об электронной подписи", который за прошлый год был дополнен существенным количеством подзаконных актов.

В прошлом году, как отмечает Мария Каншина, так и не прояснилась позиция регуляторов в организации защиты виртуальных и облачных платформ, и ожидания регулятивных действий в этой сфере переносятся на 2013-й.

В первую очередь этих действий ждут государственные организации. Так, Владимир Овчарук отмечает большой рост количества заказов на сайте государственных закупок как на проектирование и внедрение виртуализированных сред, так и на предоставление неисключительных прав на использование лицензионных средств виртуализации.

К наиболее значимым событиям 2012 г. в области государственного регулирования сферы ИБ г-жа Каншина относит вступление в силу статьи 27 "Обеспечение защиты информации в платежной системе" федерального закона № 161-ФЗ "О национальной платежной системе" (НПС). В этой связи стоит упомянуть также ряд подзаконных актов, определяющих требования к защите информации при переводе денежных средств, к обеспечению бесперебойности функционирования, к отчетности со стороны участников НПС, а также акты о контроле регуляторов в НПС.

Мария Каншина обращает внимание на жестко установленные сроки. Операторы платежных систем должны были направить регистрационное заявление в Банк России до 1 января 2013-го. Операторы по переводу денежных средств и операторы услуг платежной инфраструктуры должны представлять в Банк России сведения об ИБ-инцидентах в платежных системах ежемесячно с 14 августа 2012-го. Операторы платежных систем, операторы услуг платежной инфраструктуры, операторы по переводу денежных средств должны представить результаты оценки соответствия требованиям к обеспечению защиты информации при осуществлении переводов денежных средств в Банк России до 1 августа 2014 г. или по его требованию.

Главные споры о применении закона об НПС в прошедшем году, как отмечает г-жа Каншина, были связаны со статьей 9, вступившей в силу 1 января 2013 г. В соответствии с 4-й частью этой статьи оператор по переводу денежных средств обязан информировать клиента о совершении каждой операции с использованием электроных средств платежа, направляя ему уведомление в порядке, установленном договором. И если оператор этого не сделает, то в случае инцидента с платежом он будет обязан возместить клиенту сумму операции, о которой тот не был проинформирован (часть 13 статьи 9 закона об НПС).

Как положительный факт прошедшего года Алексей Сабанов отмечает принципиальную подвижку в отношениях между госрегуляторами и сообществами специалистов: при министерствах (Минздраве, Минкомсвязи и др.) стали создаваться экспертные и общественные советы, в том числе из специалистов, не состоящих на государственной службе. По мнению г-на Сабанова, в условиях ограниченного количества профильных специалистов в министерствах расширенное экспертное обсуждение актуальных тем может дать существенный толчок в развитии отраслевого регулирования.

Алексей Сабанов считает, что назрела необходимость создания общественного объединения основных участников российского рынка ИБ, возможно, в виде саморегулируемой организации. Он надеется, что такая организация, признанная регуляторами и работающая с ними в тесном контакте, появится в наступившем году.

По мнению Евгения Куртукова, полезным для состояния ИБ в нашей стране стало бы введение госрегуляторами требования к компаниям раскрывать информацию о преступлениях в сфере ИТ.

Государственное противодействие киберпреступности

Эксперты отмечают активизацию действий со стороны государства, направленных против киберпреступлений. Стремление правоохранительных органов и иных государственных силовых структур опережать киберпреступников активизирует применение средств слежения. Их использование актуализирует проблемы соблюдения гражданских прав и неприкосновенности тайны частной жизни. Как считают эксперты из "Лаборатории Касперского", такая ситуация обострит в обществе полемику по этому поводу.

Киберпреступность процветает в регионах с неэффективной правоохранительной системой, особенно там, где преступники могут использовать украденные средства в легальной экономике. Согласно прогнозам компании Trend Micro, следующей "тихой гаванью" для киберпреступников станет Африка.

Вместе с тем специалисты Trend Micro считают, что наступивший год является идеальным временем для принятия новых стандартов в области ИБ и для разработки новых решений с целью нанесения решающего удара по интернет-подполью. Если это произойдет, то 2013 г., по их мнению, войдет в историю как переломная точка в борьбе с киберпреступностью.

На реализацию мер по борьбе с мировой киберпреступностью в полном объеме, по оценкам экспертов из Trend Micro, потребуется не менее двух лет. Некоторые страны уже создали службы по борьбе с киберпреступностью. Вместе с тем предполагается, что в большинстве промышленно развитых стран эффективное законодательство в этой сфере будет введено не ранее 2015 г.

Россия еще может успеть пройти этот этап в ногу с развитыми государствами. Однако аналитики из российской компании Group-IB торопят тех, кто отвечает за национальную кибербезопасность. Они полагают, что если в борьбе с киберпреступностью в нашей стране не наступит качественных улучшений в течение года, то российский Интернет будет захвачен киберкриминалом, который активно двинется во власть, используя награбленные ресурсы.

Некоторые позитивные сдвиги, способные не дать реализоваться пессимистичному сценарию Group-IB, уже начались. Так, в январе 2013 г. российский президент издал указ, согласно которому ФСБ РФ поручается создать государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на российские информационные ресурсы.

ПОТРАТИВ ВСЕГО 5 МИНУТ НА ЗАПОЛНЕНИЕ АНКЕТЫ, ВЫ БУДЕТЕ БЕСПЛАТНО ПОЛУЧАТЬ PC Week/RE 50 НЕДЕЛЬ

PC WEEK RUSSIAN EDITION

КОРПОРАТИВНАЯ ПОДПИСКА

Уважаемые читатели!

Только полностью заполненная анкета, рассчитанная на руководителей, отвечающих за автоматизацию предприятий; специалистов по аппаратному и программному обеспечению, телекоммуникациям, сетевым и информационным технологиям из организаций, имеющих **более 10 компьютеров**, дает право на **бесплатную** подписку на газету PC Week/RE в течение года с момента получения анкеты. Вы также можете заполнить анкету на сайте: www.pcweek.ru/subscribe_print/.

Примечание. На домашний адрес еженедельник по бесплатной корпоративной подписке не высылается. Данная форма подписки распространяется только на территорию РФ.

Я хочу, чтобы моя организация получала PC Week/RE !

Название организации:

Почтовый адрес организации:

Индекс: Область:

Город:

Улица: Дом:

Фамилия, имя, отчество:

Подразделение / отдел:

Должность:

Телефон: Факс:

E-mail: WWW:

(Заполните анкету печатными буквами!)

1. К какой отрасли относится Ваше предприятие?

1. Энергетика ❑
2. Связь и телекоммуникации ❑
3. Производство, не связанное с вычислительной техникой (добывающие и перерабатывающие отрасли, машиностроение и т. п.) ❑
4. Финансовый сектор (кроме банков) ❑
5. Банковский сектор ❑
6. Архитектура и строительство ❑
7. Торговля товарами, не связанными с информационными технологиями ❑
8. Транспорт ❑
9. Информационные технологии (см. также вопрос 2) ❑
10. Реклама и маркетинг ❑
11. Научно-исследовательская деятельность (НИИ и вузы) ❑
12. Государственно-административные структуры ❑
13. Военные организации ❑
14. Образование ❑
15. Медицина ❑
16. Издательская деятельность и полиграфия ❑
17. Иное (что именно)

2. Если основной профиль Вашего предприятия – информационные технологии, то уточните, пожалуйста, сегмент, в котором предприятие работает:

1. Системная интеграция ❑
2. Дистрибуция ❑
3. Телекоммуникации ❑
4. Производство средств ВТ ❑
5. Продажа компьютеров ❑
6. Ремонт компьютерного оборудования ❑
7. Разработка и продажа ПО ❑
8. Консалтинг ❑
9. Иное (что именно)

3. Форма собственности Вашей организации (отметьте только один пункт)

1. Госпредприятие ❑
2. ОАО (открытое акционерное общество) ❑
3. ЗАО (закрытое акционерное общество) ❑
4. Зарубежная фирма ❑
5. СП (совместное предприятие) ❑
6. ТОО (товарищество с ограниченной ответственностью) или ООО (Общество с ограниченной ответственностью) ❑
7. ИЧП (индивидуальное частное предприятие) ❑
8. Иное (что именно)

4. К какой категории относится подразделение, в котором Вы работаете? (отметьте только один пункт)

1. Дирекция ❑
2. Информационно-аналитический отдел ❑
3. Техническая поддержка ❑
4. Служба АСУ/ИТ ❑
5. ВЦ ❑
6. Инженерно-конструкторский отдел (САПР) ❑
7. Отдел рекламы и маркетинга ❑
8. Бухгалтерия/Финансы ❑
9. Производственное подразделение ❑
10. Научно-исследовательское подразделение ❑
11. Учебное подразделение ❑
12. Отдел продаж ❑
13. Отдел закупок/логистики ❑
14. Иное (что именно)

5. Ваш должностной статус (отметьте только один пункт)

1. Директор / президент / владелец ❑
2. Зам. директора / вице-президент ❑
3. Руководитель подразделения ❑
4. Сотрудник / менеджер ❑
5. Консультант ❑
6. Иное (что именно)

6. Ваш возраст

1. До 20 лет ❑
2. 21–25 лет ❑
3. 26–30 лет ❑
4. 31–35 лет ❑
5. 36–40 лет ❑
6. 41–50 лет ❑
7. 51–60 лет ❑
8. Более 60 лет ❑

7. Численность сотрудников в Вашей организации

1. Менее 10 человек ❑
2. 10–100 человек ❑
3. 101–500 человек ❑
4. 501–1000 человек ❑
5. 1001–5000 человек ❑
6. Более 5000 человек ❑

8. Численность компьютерного парка Вашей организации

1. 10–20 компьютеров ❑
2. 21–50 компьютеров ❑
3. 51–100 компьютеров ❑
4. 101–500 компьютеров ❑
5. 501–1000 компьютеров ❑
6. 1001–3000 компьютеров ❑
7. 3001–5000 компьютеров ❑
8. Более 5000 компьютеров ❑

9. Какие ОС используются в Вашей организации ?

1. DOS ❑
2. Windows 3.xx ❑
3. Windows 9x/ME ❑
4. Windows NT/2K/XP/2003 ❑
5. OS/2 ❑
6. Mac OS ❑
7. Linux ❑
8. AIX ❑
9. Solaris/SunOS ❑
10. Free BSD ❑
11. HP/UX ❑
12. Novell NetWare ❑
13. OS/400 ❑
14. Другие варианты UNIX ❑
15. Иное (что именно)

10. Коммуникационные возможности компьютеров Вашей организации

1. Имеют выход в Интернет по выделенной линии ❑
2. Объединены в intranet ❑
3. Объединены в extranet ❑
4. Подключены к ЛВС ❑
5. Не объединены в сеть ❑
6. Dial Up доступ в Интернет ❑

11. Имеет ли сеть Вашей организации территориально распределенную структуру (охватывает более одного здания)?

Да ❑ Нет ❑

12. Собирается ли Ваше предприятие устанавливать интрасети (intranet) в ближайший год ?

Да ❑ Нет ❑

13. Сколько серверов в сети Вашей организации ?

14. Если в Вашей организации используются мэйнфреймы, то какие именно?

1. ЕС ЭВМ ❑
2. IBM ❑
3. Unisys ❑
4. VAX ❑
5. Иное (что именно)
6. Не используются ❑

15. Компьютеры каких фирм-изготовителей используются на Вашем предприятии?

	Настольные ПК	Портативные ПК	Серверы
"Аквариус"	❑	❑	❑
ВИСТ	❑	❑	❑
"Формоза"	❑	❑	❑
Acer	❑	❑	❑
Apple	❑	❑	❑
CLR	❑	❑	❑
Compaq	❑	❑	❑
Dell	❑	❑	❑
Fujitsu Siemens	❑	❑	❑
Gateway	❑	❑	❑
Hewlett-Packard	❑	❑	❑
IBM	❑	❑	❑
Kraftway	❑	❑	❑
R.&K.	❑	❑	❑
R-Style	❑	❑	❑
Rover Computers	❑	❑	❑
Sun	❑	❑	❑
Siemens Nixdorf	❑	❑	❑
Toshiba	❑	❑	❑

Иное (что именно)

16. Какое прикладное ПО используется в Вашей организации?

1. Средства разработки ПО ❑
2. Офисные приложения ❑
3. СУБД ❑
4. Бухгалтерские и складские программы ❑
5. Издательские системы ❑
6. Графические системы ❑
7. Статистические пакеты ❑
8. ПО для управления производственными процессами ❑
9. Программы электронной почты ❑
10. САПР ❑
11. Браузеры Internet ❑
12. Web-серверы ❑
13. Иное (что именно)

17. Если в Вашей организации установлено ПО масштаба предприятия, то каких фирм-разработчиков?

1. "1С" ❑
2. "АйТи" ❑
3. "Галактика" ❑
4. "Парус" ❑
5. BAAN ❑
6. Navision ❑
7. Oracle ❑
8. SAP ❑
9. Epicor Scala ❑
10. ПО собственной разработки ❑
11. Иное (что именно)
12. Не установлено никакое ❑

18. Существует ли на Вашем предприятии единая корпоративная информационная система?

Да ❑ Нет ❑

19. Если Ваша организация не имеет своего Web-узла, то собирается ли она в ближайший год завести его?

Да ❑ Нет ❑

20. Если Вы используете СУБД в своей деятельности, то какие именно?

1. Adabas ❑
2. Cache ❑
3. DB2 ❑
4. dBase ❑
5. FoxPro ❑
6. Informix ❑
7. Ingress ❑
8. MS Access ❑
9. MS SQL Server ❑
10. Oracle ❑
11. Progress ❑
12. Sybase ❑
13. Иное (что именно)
14. Не используем ❑

21. Как Вы оцениваете свое влияние на решение о покупке средств информационных технологий для своей организации? (отметьте только один пункт)

1. Принимаю решение о покупке (подписываю документ) ❑
2. Составляю спецификацию (выбираю средства) и рекомендую приобрести ❑
3. Не участвую в этом процессе ❑
4. Иное (что именно)

22. На приобретение каких из перечисленных групп продуктов или услуг Вы оказываете влияние (покупаете, рекомендуете, составляете спецификацию)?

Системы

1. Мэйнфреймы ❑
2. Миникомпьютеры ❑
3. Серверы ❑
4. Рабочие станции ❑
5. ПК ❑
6. Тонкие клиенты ❑
7. Ноутбуки ❑
8. Карманные ПК ❑

Сети

9. Концентраторы ❑
10. Коммутаторы ❑
11. Мосты ❑
12. Шлюзы ❑
13. Маршрутизаторы ❑
14. Сетевые адаптеры ❑
15. Беспроводные сети ❑
16. Глобальные сети ❑
17. Локальные сети ❑
18. Телекоммуникации ❑

Периферийное оборудование

19. Лазерные принтеры ❑
20. Струйные принтеры ❑
21. Мониторы ❑
22. Сканеры ❑
23. Модемы ❑
24. ИБП (UPS) ❑

Память

25. Жесткие диски ❑
26. CD-ROM ❑
27. Системы архивирования ❑
28. RAID ❑
29. Системы хранения данных ❑

Программное обеспечение

30. Электронная почта ❑
31. Групповое ПО ❑
32. СУБД ❑
33. Сетевое ПО ❑
34. Хранилища данных ❑
35. Электронная коммерция ❑
36. ПО для Web-дизайна ❑
37. ПО для Интернета ❑
38. Java ❑
39. Операционные системы ❑
40. Мультимедийные приложения ❑
41. Средства разработки программ ❑
42. CASE-системы ❑
43. САПР (CAD/CAM) ❑
44. Системы управления проектами ❑
45. ПО для архивирования ❑

Внешние сервисы

46. ❑

Ничего из вышеперечисленного

47. ❑

23. Каков наивысший уровень, для которого Вы оказываете влияние на покупку компьютерных изделий или услуг (служб)?

1. Более чем для одной компании ❑
2. Для всего предприятия ❑
3. Для подразделения, располагающегося в нескольких местах ❑
4. Для нескольких подразделений в одном здании ❑
5. Для одного подразделения ❑
6. Для рабочей группы ❑
7. Только для себя ❑
8. Не влияю ❑
9. Иное (что именно)

24. Через каких провайдеров в настоящее время Ваша фирма получает доступ в интернет и другие интернет-услуги?

1. "Демос" ❑
2. МТУ-Интел ❑
3. "Релком" ❑
4. Combellga ❑
5. Comstar ❑
6. Golden Telecom ❑
7. Equant ❑
8. ORC ❑
9. Telmos ❑
10. Zebra Telecom ❑
11. Через других (каких именно)

Дата заполнения

Отдайте заполненную анкету представителям PC Week/RE либо пришлите ее по адресу: **109147, Москва, ул. Марксистская, д. 34, корп. 10, PC Week/RE.**

Анкету можно отправить на e-mail: info@pcweek.ru

SEMAT — вторая революция в программной инженерии?

СЕРГЕЙ БОБРОВСКИЙ

Программная инженерия как официальная дисциплина родилась в 1968 г. на конференции НАТО в немецком Гармише, когда военные признали необходимость серьезных инвестиций в исследования по созданию крупных программных проектов. Уже в то время реализовывались проекты, по масштабам не так и сильно отличавшиеся от нынешних: например, еще в 1957 г. компьютер IBM SAGE AN/FSQ-7 управлял в реальном времени стратегической системой противоракетной обороны США, обрабатывая данные от десятков радарных установок.

40 лет блуждания в темноте

Официально признанное направление, однако, практически так и не породило ожидаемых сильных идей, которые удалось бы успешно воплотить на практике. Разрозненные конференции и единичные семинары затерялись в вале неудачных ИТ-проектов. Каждое десятилетие дополнительные накладные расходы на разработку и внедрение ПО вырастают на треть, да и по сей день эта тенденция не меняется. К 1980-м годам, в разгар холодной войны на фоне повсеместной корпоративной автоматизации и связываемых с нею радужных перспектив, ситуация стала особо критичной — затягивание сроков, перерасходы бюджетов и количество ошибок в программах превышали все мыслимые границы. Поэтому в 1986 г. МО США создало официальную структуру — институт программной инженерии SEI при Университете Карнеги — Меллона, который и сегодня большую часть бюджета получает от военных. С тех пор едва ли не самая активная научно-практическая деятельность по этому профилю ведется в SEI, а результатом ее стала, в частности, модель зрелости программных процессов Capability Maturity Model (CMM). Разработал ее Уотс Хамфри, пришедший в SEI из IBM, где занимал должность вице-президента. CMM оказалась, пожалуй, наиболее успешным на сегодня достижением программной инженерии. Так, большинство федеральных структур США, реализующих крупные ИТ-проекты, должны иметь сертификат CMM.

Однако "серебряной пули" из CMM не получилось. Эта модель сложна в реализации, рассчитана на крупные организации, а опыт ее использования плохо переносится даже между подразделениями одной компании. В результате Хамфри разработал интеграционный вариант Capability Maturity Model Integration, который, впрочем, тоже не удалось успешно подстроить под достижения набравшего популярность движения agile-разработки. Однако никаких других альтернатив CMM в первом десятилетии XXI века не появилось.

Духовные наследники CMM

В декабре 2009-го заработала организация Software Engineering Method and Theory (SEMAT), созданная Айваром Якобсоном, одним из основных разработчиков языка моделирования UML, методологии RUP и технологии аспектно-ориентированного программирования; Бертраном Мейером, создателем языка программирования Eiffel и концепции контрактной разработки; Ричардом Соли, CEO консорциума OMG по развитию объектно-ориентированных стандартов и технологий. В марте 2010-го в Цюрихе состоялся первый массовый семинар SEMAT. На нем Уотс Хамфри сравнил данный семинар в плане его исторической значимости для программной инженерии с мероприятием НАТО 1968 г.! Что же так впечатлило автора CMM в очередном творении коллег по программному цеху?

Разобраться в этом помогла состоявшаяся 20 декабря конференция, посвященная открытию Российского отделения SEMAT. Вел ее хорошо известный отечественным специалистам по программной инженерии д-р техн. наук Борис Позин, технический директор компании "ЕС-лизинг", организовавшей это мероприятие. С рассказом о перспективах SEMAT в режиме телеприсутствия выступил Айвар Якобсон.

20 лет назад программная инженерия развивалась "под эгидой" объектно-ориентированного программирования; 15 лет назад популярными стали RUP и UML; 12 лет назад получила массовое признание во всем мире модель CMM; сегодня пользуются спросом agile-практики наподобие Scrum и Kanban. Однако единой успешной и универсальной концепции разработки ПО в срок, в рамках бюджета и с надлежащим качеством так и не появилось.

Хотя с известной даты прошло более 40 лет, отрасль программной инженерии все еще молода, и незрелые практики по-прежнему присутствуют в массовом порядке даже в самых крупных компаниях. Профессионалы не умеют быстро переносить свои навыки в другие проекты. Улучшение процессов производства ПО в крупных организациях трудоемко, а сами процессы несовместимы друг с другом — от "канбана" к "скраму" не перебежишь. Что касается обучения, то, говоря программистским языком, люди учатся конкретным "экземплярам" методов (Scrum, RUP) вместо освоения универсальной методологической базы. Сохраняется разрыв между академическими и прикладными наработками.

Сегодняшняя индустрия ПО характеризуется избыточным количеством подходов и инструментов, часто выполняется пустая работа по созданию "новых" технологий разработки, а методологи конкурируют друг с другом, вместо того чтобы сотрудничать. Всем нынешним подходам не хватает прежде всего глубокого фундамента, и именно эту проблему решает SEMAT — входящие в это сообщество гуру пытаются сделать все процессы производства софта точно измеряемыми и выполненными на хорошем математическом базисе. Предлагаемый SEMAT продукт должен будет работать независимо от конкретных методологий, технологий и инструментов. Его ядро (так называемый мета-метод) включает средства анализа прогресса проекта, состояния и функциональности создаваемой системы. Якобсон отметил, что фактически SEMAT подсказывает, куда из текущего проектного состояния идти не надо, дабы не оказаться в проигрышной ситуации ("умрет ли проект?"). В продукт входят четыре "версии": для уже производящих программный продукт и для планирующих, для сопровождения ПО и для исследований и обучения.

Ближайшие 40 лет — под эгидой SEMAT

Такой тезис прозвучал на мероприятии, и на это имеются определенные основания. К SEMAT уже присоединилось 1784 участника, включая Барри Боэма, автора COCOMO (модель оценки стоимости разработки ПО), Эриха Гамму, Эда Йордона, Джонса Каперса (модель функциональных точек). По понятным причинам SEMAT активно поддерживается консорциумом OMG. В деятельности SEMAT участвуют Ericsson, Fujitsu, IBM, Microsoft, Samsung, институты программной инженерии Швеции, Южной Кореи, Китая. Интересно, что уже семь из первой десятки китайских вузов официально поддержали SEMAT-инициативу.

На сайте semat.org доступно немало методических материалов, имеется книга "The Essence of Software Engineering: Applying the SEMAT Kernel". Приятно, что в работе SEMAT принимают участие и отечественные специалисты: помимо Бориса Позина, пока выступающего координатором Российского отделения SEMAT, виртуально присутствовавший на мероприятии Андрей Байда из Санкт-Петербурга входит в рабочую группу по разработке теории SEMAT. Участвует в инициативе SEMAT и профессор Андрей Терехов, директор НИИ информационных технологий СПбГУ.

В первой половине 2013 г. российское отделение SEMAT, будем надеяться, сформируется в активно действующую структуру со своим интернет-представительством, в работе которого смогут участвовать все желающие. PC Week/RE будет информировать читателей об этом перспективном проекте.