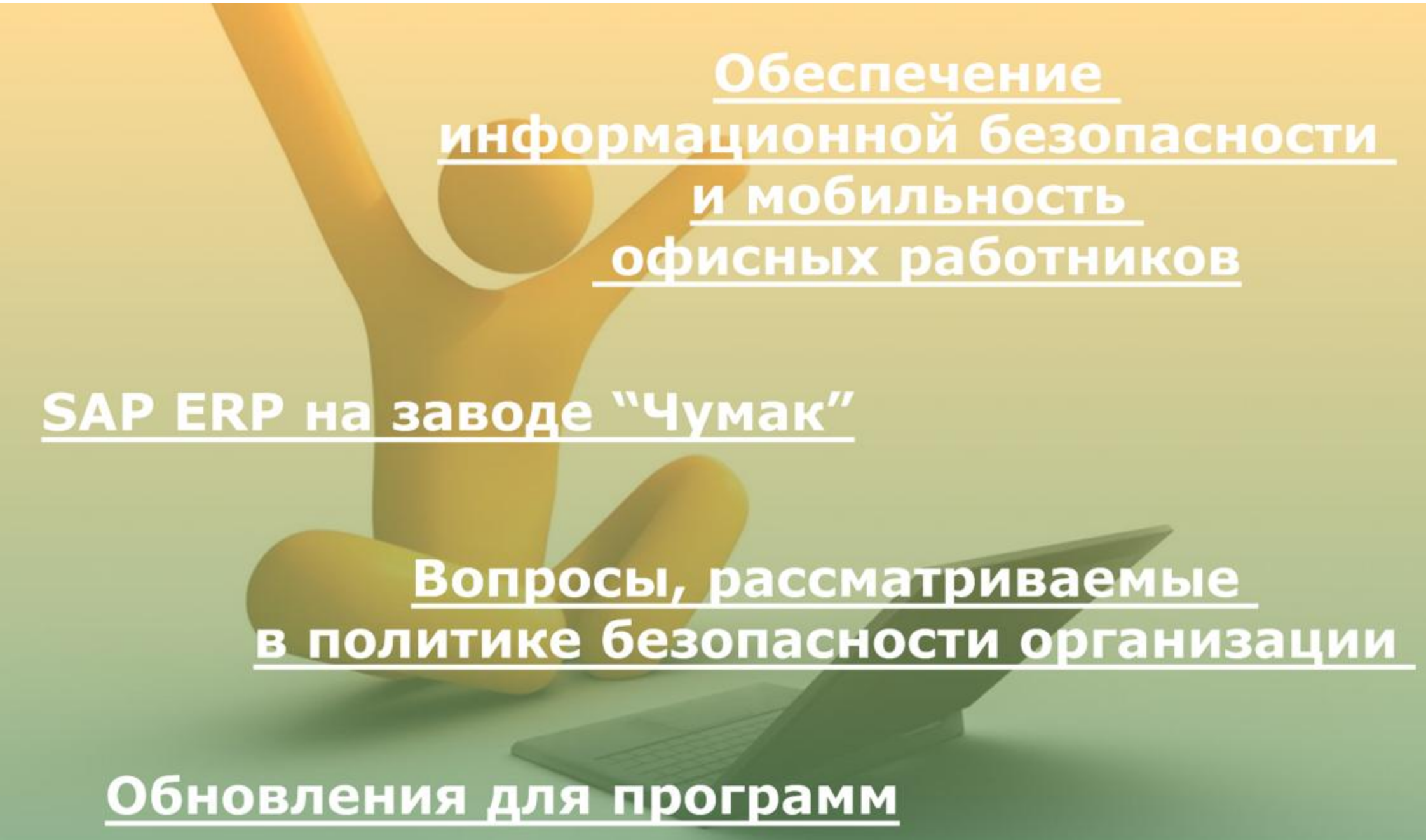
KV.BIZ КОМПЬЮТЕРНЫЕ ВЕСТИ
www.kv.by
No. 004 (9)
21 июня 2013 года
ООО "РГ "Компьютерные Вести" • Тираж: 11283 экз. • Адрес: Минск, ул. Мельникайте, 2, оф. 710 • E-mail: info@kv.by • Тел. редакции (017) 203-90-10 • Размещение рекламы: adv@kv.by



Обеспечение информационной безопасности и мобильность офисных работников

SAP ERP на заводе "Чумак"

Вопросы, рассматриваемые в политике безопасности организации

Обновления для программ

Обеспечение информационной безопасности в связи с мобильностью офисных работников

Роман ИДОВ, ведущий аналитик компании SearchInform

Сегодня бизнес требует от своих работников мобильности. И для этого сотрудники используют мобильные устройства — вряд ли сегодня есть компании, где никто не пользуется ноутбуками, планшетами, смартфонами. Но их использование негативно сказывается на состоянии информационной безопасности компаний.

Консьюмеризация шагает по планете

Все мы живем в обществе потребления и что-то потребляем, но в данном случае термин "комсьюмеризация" связан с этим не совсем напрямую. Тем не менее, проблема эта более чем актуальна во всем мире, и постсоветское пространство — не исключение.

Исследование компании Dimensional Research, проведенное по заказу Dell, показало, что уже 87% компаний практикуют использование своими сотрудниками личных устройств в рабочих целях. Причем это оказываются не только смартфоны (которые используются в 80% компаний), но и портативные компьютеры (в 69% компаний), включая и такие популярные сегодня планшетные ПК.

Думаю, все знают, что одной из наиболее важных проблем, связанных с использованием личных устройств, является обеспечение защиты корпоративных данных от утечек. Эта проблема действительно масштабна: 64% ИТ-специалистов отмечает, что не могут контролировать все устройства, подключаемые к корпоративной сети. Исследования компании SearchInform показали, что около 80% компаний, разрешающих сотрудникам пользоваться собственными портативными устройствами на рабочем месте, даже не задумывались о необходимости контролировать их.

К сожалению, в большинстве случаев подобные проблемы решают традиционным "не пущать и запрещать", в то время как было бы гораздо эффективнее контролировать использование сотрудниками собственных устройств. Об этом мы сейчас немного и поговорим.

Почему запрещать плохо?

На Западе чрезвычайно популярна концепция BYOD — Bring Your Own Device. Работники пользуются приобретенными ими самими устройствами, работодатель экономит на их покупке, при этом довольны обе стороны, при условии соблюдения соответствующих мер контроля.

Почему бы просто не запретить использование собственных устройств сотрудниками? Во-первых, само по себе приобретение лэптопов или планшетов за корпоративный счет не дает никаких гарантий безопасности. Работник может точно так же пользоваться устройством дома, в кафе, на вокзале, может точно так же потерять его. Во-вторых, никто не мешает сотруднику, получив корпоративный планшет, пользоваться параллельно и собственным. Или, если у него уже есть собственный, корпоративный может быть просто спрятан в ящик рабочего стола.

То есть, проблема именно в неэффективности подобных запретительных мер. В тоже время контроль устройств будет куда более удачным и удобным решением.

Контроль лэптопов

Это самый простой аспект наведения порядка в использовании работниками личных устройств. Поскольку о нем уже рассказывалось, подробно повторяться не вижу необходимости, хотя пару слов всё-таки сказать стоит.

Многие современные DLP-системы имеют в своем составе endpoint-модуль, который может функционировать независимо от подключения ноутбука или нетбука к корпоративной сети. В таком режиме модуль собирает информацию, которая при подключении к сети компании передается для анализа серверной части решения.

Контроль планшетов и смартфонов

Планшетные ПК тоже можно контролировать подобным образом, но пока модули для этого есть далеко не во всех DLP-системах. В настоящее время наиболее актуален контроль устройств под управлением iOS, но в ближайшее время также может стать актуальным и контроль устройств на базе ОС Android.

Но в случае с планшетами всё-таки более важно контролировать их работу именно в корпоративной сети. Для этого движение перехваченного трафика осуществляется через VPN-сервер, на котором установлен агент с уникальной конфигурацией. Полученные с мобильного устройства данные передаются серверу управления, производится их обработка, размещение в базы данных, индексирование и проверка по настроенным политикам безопасности на предмет утечки конфиденциальной информации.

Аналогичным образом реализуется и контроль другого популярного класса устройств — смартфонов.

Насколько это эффективно

Как показывают исследования компании SearchInform, применение подобных мер контроля по отношению к устройствам сотрудников позволяет сократить количество утечек информации в среднем на 35%, что, согласитесь, весьма немало с учетом того, что каждая утечка сегодня стоит уже более 5 млн. долларов.

Обсудить

Вопросы, рассматриваемые в политике безопасности организации

Владимир БЕЗМАЛЫЙ, vladb@windowslive.com,
специалист по обеспечению безопасности,
MVP Consumer Security, Microsoft Security Trusted Advisor

Сегодня практически каждая крупная компания создает свое подразделение защиты информации. Трудно себе представить фирму, которая всерьез озабочена состоянием своей информационной безопасности, но не хочет создавать соответствующее подразделение. Перед отделом (департаментом) защиты информации рано или поздно встает вопрос написания политики защиты информации. Но тут же встает и другой вопрос, а именно, что же должно быть в этой политике? На этот вопрос я и постараюсь ответить в своей статье.

Предположим, что у нас есть некая компания X и мы предлагаем те вопросы, которые необходимо рассмотреть в политике безопасности:

– Роль информации и информационных систем Компании.

– Какие системы вовлекаются в политику безопасности?

– Основные подразделения, работающие в области защиты информации

– Категорирование сотрудников

– Классификация информации

– Маркирование информации

– Политика учетных записей

– Пользовательское соглашение

– Требования к партнерам (третьим сторонам)

– Физическая безопасность

– Внутренние сетевые подключения

– Внешние сетевые подключения

– Изменения в топологии сети

– Доступ к Internet

– Порядок работы с электронной почтой

– Защита от вирусов

– Резервное копирование

– Письменные спецификации ПО

– Право мониторинга

– Роль информации и информационных систем Компании.

Компания X критически зависит от информации и информационных систем. Если важная информация будет раскрыта несоответствующим лицам, компания понесет серьезные потери или будет признана банкротом. Хорошая репутация, которой пользуется Компания X, также непосредственно связана со способом управления информацией и информационными системами. Например, если бы частная информация клиента была бы публично раскрыта, репутация организации понесла бы урон. По этим и другим важным причинам, Правление компании, работающее вместе с Советом директоров, инициализировало и продолжает поддерживать мероприятия по защите информации. Одно из таких мероприятий — определение политики информационной безопасности.

Информационная безопасность — дело каждого!

Чтобы быть эффективной, информационная безопасность должна быть общим усилием, делом каждого работника, имеющего дело с информацией и информационными системами. С учетом потребности во взаимодействии, эта политика разъясняет обязанности пользователей и их обязанности по защите информации и информационных систем. Политика безопасности описывает способы предотвращения и ответы на разнообразие угроз информации и информационным системам, включая несанкционированный доступ, раскрытие, дублирование, модификацию, разрушение, потерю, неправильное употребление, и отрицание использования. Отсюда вытекает следующий вопрос.

Для кого предназначена политика безопасности?

Каждый работник должен исполнять политику информационной безопасности. Сотрудники, преднамеренно нарушающие Политику информационной безопасности, должны быть привлечены к дисциплинарному воздействию, включая возможное увольнение. Какие системы вовлекаются в политику безопасности? Политика применяется ко всем компьютерным и сетевым системам, принадлежащим или управляемым Компанией X. Данная политика применяется ко всем операционным системам, компьютерам и прикладным системам. Политика охватывает только информацию, обрабатываемую компьютерами и сетями. Хотя Политика безопасности включает упоминание о других способах обработки информации типа голосового и бумажного, однако непосредственно не оговаривает методы защиты информации при таких методах обработки. Для информации о защите информации в бумажной форме создается отдельный документ. Основные подразделения, работающие в области защиты информации Невзирая на то, что информационной безопасностью в компании в той или иной мере заняты все сотрудники, руководство и полномочия по защите информации централизованы для всей Компании X, и сосредоточены в Отделе защиты информации. Данный отдел отвечает за разработку, внедрение и поддержку политики информационной безопасности, стандартов, рекомендаций и процедур для всей организации. Проверка соответствия для гарантии

Вопросы, рассматриваемые в политике безопасности организации

Итого, что организационные модули работают способом, совместимым с этими требованиями возлагается на подразделение Аудита Информационных технологий, состоящего в штате Отдела Внутреннего Аудита.

Дисциплинарные вопросы, следующие из нарушений требований информационной безопасности должны отрабатываться менеджерами, работающими вместе с отделом кадров. Категорирование сотрудников Чтобы координировать командные усилия, Компания X должна установить три категории работников. При этом каждый сотрудник может относиться не менее чем кодной из них. Это следующие категории — Владелец, Хранитель, и Пользователь. Эти категории определяют общие обязанности по отношению к требованиям информационной безопасности. На данном этапе сотрудникам службы информационной безопасностинеобходимо разобраться со схемами прохождения и обработки информации в компании и выяснить кому принадлежит какая информация.

Владелец информации

К данной категории относятся менеджеры, члены группы высшего исполнительного руководства, которые несут ответственность за приобретение, развитие, и обслуживание приложений, обрабатывающих информацию, принадлежащую Компании X. Для каждого типа информации, Владельцы определяют уместную классификацию информации, определяют соответствующий уровень критичности, определяют, каким пользователям будет предоставлен доступ, одобряют запросы о различных путях использования информации. При этом вся информация прикладной системы должна иметь определенного Владельца.

Хранители информации

К данной категории относятся сотрудники, которые отвечают за сохранность информации, принадлежащей компании X. Естественно, что сотрудники подразделения ИТ являются Хранителями, но, в, то же время, и пользователи, в момент, когда информация находится на их рабочих станциях, тоже являются Хранителями. Каждый тип информации прикладной системы должен иметь одного или более определяемых Хранителей. Хранители отвечают за сохранность информации, включая осуществление систем управления доступом, чтобы предотвратить несоответствующее раскрытие, и за создание резервных копий таким образом, чтобы критичная информация не была потеряна. Хранители также обязаны осуществлять, использовать, и поддерживать меры безопасности, определенные Владельцами информации.

Обязанности пользователей

Пользователи обязаны ознакомиться с политикой информационной безопасности (в части их касающейся) под роспись. Они отвечают за исполнение политики, процедур и стандартов информационной безопасности. При этом все вопросы по обработке определенного типа информации должны быть направлены или Хранителю или Владельцу соответствующей информации.

Защита информации на всем ее жизненном цикле

Информация, принадлежащая компании X, и информация, которая была поручена к обработке Компании X, должна быть защищена способом, соразмерным ее чувствительностью и критичностью. Меры защиты должны использоваться независимо относителей, на которых информация сохранена, систем, которые ее обрабатывают, или методов, которыми она обрабатывается. Информация должна быть защищена способом, который является совместимым с ее классификацией на всем периоде ее существования, от разработки (происхождения) до разрушения. Классификация информации Согласно требований украинского законодательства, владелец информации вправе сам определить степень конфиденциальности обрабатываемой информации, если иное не определено законом. Исходя из необходимости обеспечения различных уровней защиты разных видов информации (не содержащей сведений, составляющих государственную тайну), хранимой и обрабатываемой в автоматизированной системе, в Компании X вводится несколько категорий конфиденциальности и целостности защищаемой информации, а также категории решаемых задач.

Категории конфиденциальности защищаемой информации

– “СТРОГО КОНФИДЕНЦИАЛЬНАЯ” — к данной категории относится информация, являющаяся конфиденциальной в соответствии с требованиями действующего законодательства (банковская тайна), а также информация, ограничения на распространение которой введены решениями руководства организации (коммерческая тайна), разглашение которой может привести к тяжким финансово-экономическим последствиям для организации вплоть до банкротства (нанесению тяжкого ущерба жизненно важным

Вопросы, рассматриваемые в политике безопасности организации

интересам его клиентов, корреспондентов, партнеров или сотрудников);

– "КОНФИДЕНЦИАЛЬНАЯ" — к данной категории относится информация, не отнесенная к категории "СТРОГО КОНФИДЕНЦИАЛЬНАЯ", ограничения на распространение которой вводятся решением руководства организации в соответствии с предоставленными ему как собственнику (уполномоченному собственником лицу) информации действующим законодательством правами, разглашение которой может привести к значительным убыткам и потере конкурентоспособности организации (нанесению ощутимого ущерба интересам его клиентов, корреспондентов, партнеров или сотрудников);

– "ОТКРЫТАЯ" — к данной категории относится информация, обеспечения конфиденциальности (введения ограничений на распространение) которой не требуется. Категории целостности защищаемой информации

– "ВЫСОКАЯ" — к данной категории относится информация, несанкционированная модификация (искажение, подмена, уничтожение) или фальсификация (подделка) которой может привести к нанесению значительного прямого ущерба организации, целостность и аутентичность (подтверждение подлинности источника) которой должна обеспечиваться гарантированными методами (средствами электронной цифровой подписи — ЭЦП) в соответствии с обязательными требованиями действующего законодательства, приказов, директив и других нормативных актов;

– "НИЗКАЯ" — к данной категории относится информация, несанкционированная модификация, подмена или удаление которой может привести к нанесению незначительного косвенного ущерба организации, ее клиентам, партнерам или сотрудникам, целостность которой должна обеспечиваться в соответствии с решением руководства (методами подсчета контрольных сумм, хеш-функций);

– "НЕТ ТРЕБОВАНИЙ" — к данной категории относится информация, к обеспечению целостности (и аутентичности) которой требований не предъявляется.

Категории функциональных задач

В зависимости от периодичности решения функциональных задач и максимально допустимой задержки получения результатов их решения вводится четыре требуемых степени (категории) доступности функциональных задач. Требуемые степени доступности функциональных задач:

– "БЕСПРЕПЯТСТВЕННАЯ ДОСТУПНОСТЬ" — доступ к задаче должен обеспечиваться в любое время (задача решается постоянно, задержка получения результата не должна превышать нескольких секунд или минут);

– "ВЫСОКАЯ ДОСТУПНОСТЬ" — доступ к задаче должен осуществляться без существенных временных задержек (задача решается ежедневно, задержка получения результата не должна превышать нескольких часов);

– "СРЕДНЯЯ ДОСТУПНОСТЬ" — доступ к задаче может обеспечиваться с существенными временными задержками (задача решается раз в несколько дней, задержка получения результата не должна превышать нескольких дней);

– "НИЗКАЯ ДОСТУПНОСТЬ" — временные задержки при доступе к задаче практически не лимитированы (задача решается с периодом в несколько недель или месяцев, допустимая задержка получения результата — несколько недель).

Весь персонал Компании Х должен быть ознакомлен с определениями для этих категорий, списком категорийности информации (в части касающейся) и шагов по защите информации, относящейся к каждой из этих категорий (в части касающейся). Персонал подразделения ИТ должен быть ознакомлен под роспись (в части касающейся) со списком степеней доступности функциональных задач.

Политика защиты информации является информацией, которая относится к категории "Строго конфиденциально" или "Конфиденциально".

Приложением к данному разделу должны служить документы, определяющие категорирование информации и списком степеней доступности функциональных задач.

Маркирование информации

Большинство информации, принадлежащей Компании Х относится к категории "Конфиденциально". По этой причине, не следует применять метку "Конфиденциально". Информация без метки по умолчанию относится к данной категории.

Доступ к информации

Доступ к информации, которой владеет или которой управляет Компания Х, должен быть предоставлен только тому персоналу, которому необходимо быть с ней ознакомленным в силу служебных обязанностей. Информация может быть раскрыта только тем людям, которые имеют на это законное право. В то же самое время, персонал не должен отказать в доступе к информации, в случае если Владелец информации принял решение о ее доступности. Чтобы осуществлять концепцию необходимости, Компания Х приняла запрос на доступ к информации и процесс одобрения данного запроса Владельцем. Сотрудники не должны пытаться обратить-

Вопросы, рассматриваемые в политике безопасности организации

ся к чувствительной информации, если соответствующий Владелец не предоставил им права доступа. Когда сотрудник меняет режим работы, включая окончание работы, продвижение по службе или отпуск, его руководитель должен немедленно уведомить об этом Отдел защиты информации. Привилегии, предоставленные всем сотрудникам должны периодически пересматриваться Владельцами и Хранителями информации, чтобы гарантировать, что только те сотрудники имеют доступ, кому это требуется в силу выполняемых служебных обязанностей. В данном разделе сотрудники службы информационной безопасности должны попытаться отразить следующие моменты:

1. Как предоставляется доступ к информации? Ответом на данный вопрос должна являться “Инструкция о порядке предоставления доступа к информации”. Политика учетных записей Компании X требует, чтобы каждый сотрудник, обращающийся к многопользовательским информационным системам, имел уникальный пользовательский идентификатор (учетную запись) и собственный пароль. Эти учетные записи должны использоваться, чтобы ограничить системные привилегии, основанные на режимах работы. Каждый сотрудник несет личную ответственность за использование своей учетной записи и своего пароля. Анонимные пользовательские учетные записи ЗА ИСКЛЮЧЕНИЕМ электронных досок объявлений, сайтов Internet, сайтов intranet, и других систем, где все пользователи должны быть анонимными, запрещена регистрация анонимных пользователей в любых сетях или системах Компании X.

2. Использование сложных пользовательских паролей. Пользователи должны выбрать сложные пароли. Это означает, что пароли не должны быть связаны с работой или личной жизнью. Например, не должны использоваться номер паспорта, имя супруга (супруги), имена детей или фрагменты адреса. Это также означает, что пароли не должны быть словом, которое можно найти в словаре или некоторой другой части речи. Например, не должны использоваться имена собственные, места, технические сроки и сленг.

3. Легко запоминаемые пароли. Пользователи могут выбрать легко запоминаемые пароли, которые являются в то же самое время трудными для неправомочных сторон если они: собирают несколько слов вместе; сдвигают слово, вниз, влево, или вправо на одну строку на клавиатуре; символы, набираемые в слове на клавиатуре, сдвинуты на несколько символов вверх или вниз по алфавиту; преобразовывают правильное слово согласно определенного метода, типа сдвига по алфавиту каждого следующего символа на число, отражающее его позицию в слове; объединяют пунктуацию или числа с правильным словом; создают акронимы от слов в песне, поэме, или другой известной последовательности слов; преднамеренно делают орфографические ошибки в слове; объединяют несколько предпочтений подобно любимым цветам, предпочитаемым фильмам и т.д.

4. Требование неповторяемости паролей. Пользователи не должны создавать пароли с основной последовательностью символов, которая частично изменяется на некий предсказуемый фактор. Пользователи не должны создать пароли, которые являются идентичными или существенно подобными паролям, которые они использовали перед этим. Длина Пароля Пароль должен быть не менее 10 символов длиной. Пароли должны изменяться каждые 42 дня (рекомендация Microsoft) или чаще. Всякий раз, когда сотрудник подозревает, что его пароль скомпрометирован (стал известен другому человеку), пароль должен быть немедленно изменен.

5. Хранение паролей. Пароли не должны быть сохранены в читаемой форме в пакетных файлах, автоматических сценариях входа в систему, программных макросах, оконечных функциональных клавишах, в виде файлов в компьютерах без систем управления доступом, или в других местах, где их могли бы обнаружить злоумышленники. Пароли не могут быть записаны в некоторой разборчивой форме и оставлены в местах, где злоумышленники могли бы обнаружить и ознакомиться с ними. Совместно используемые пароли Если сотрудники совместно используют компьютерные данные, они должны использовать электронную почту, базы данных программного обеспечения для совместной работы, общие каталоги на серверах локальной сети и другие механизмы. Хотя пользовательские идентификаторы разделены для электронной почты и других целей, пароль сотрудника никогда не должен совместно использоваться или показываться другим сотрудникам. Системные администраторы и другой технический штат информационных систем никогда не должны просить о том, чтобы сотрудник показал его личный пароль. Пароль может быть известен другому сотруднику лишь при первоначальном вводе учетной записи. Эти временные пароли должны быть изменены при первом обращении уполномоченного пользователя к системе. Если пользователь считает, что его пользовательский идентификатор и пароль используются кем-то еще, он должен немедленно уведомить системного администратора информационной системы для смены пароля. Итогом данного раздела должны стать две инструкции: “О порядке именования учетных записей пользователей”, “Инструкция о парольной защите в компании”.

Пользовательское соглашение

Все сотрудники, желающие использовать компьютерные системы, принадлежащие Компании X, должны подписать пользовательское соглашение до того, как получат имя учетной записи. Если пользователи уже имеют учетные записи, они обязаны подписать пользовательское соглашение до получения ежегодно

Вопросы, рассматриваемые в политике безопасности организации

возобновляемых пользовательских идентификаторов. Подпись на этом соглашении указывает, что пользователь понимает и соглашается придерживаться политики и процедур Компании X, связанных с компьютерами и сетями, включая инструкции, которые ссылаются на эти политики (процедуры).

Требования к партнерам (третьим сторонам)

Если информация не определялась как публичная, то она должна быть защищена от раскрытия третьим лицам. Третьи лица могут получить доступ к внутренней информации Компании X только когда существует очевидная потребность и было подписано соглашение о неразглашении.

Сторонние запросы об информации

Если сотрудник не был уполномочен Владельцем информации об ее обнародовании, то все запросы для получения информации о Компании X и ее бизнесе, должны быть переданы в отдел связей с общественностью. Такие запросы включают анкетные опросы, обзоры, и газетные интервью. Этот раздел Политики не относится к информации маркетинга об изделиях и услугах Компании X. Дополнением к данному разделу должна служить "Инструкция о порядке обнародования информации".

Физическая безопасность

Доступ к каждому офису или рабочему месту, на котором обрабатывается конфиденциальная информация, должен быть физически ограничен и предоставлен только тем людям, которым необходимо знать данную информацию. Если конфиденциальная информация не используется, она всегда должна быть защищена от неправомочного раскрытия. Конфиденциальная информация в бумажной форме должна храниться в сейфах. Сотрудники должны размещать экраны компьютеров таким образом, чтобы предотвратить несанкционированный просмотр конфиденциальной информации.

Внутренние сетевые подключения

Все компьютеры Компании X, на которых обрабатывается конфиденциальная информация и которые постоянно или периодически подключены к внутренним компьютерным сетям, должны иметь систему управления доступом на основе пароля (сертификата), одобренную отделом защиты информации. Независимо от наличия сетевых подключений, все автономные компьютеры, обрабатывающие конфиденциальную информация должны также использовать одобренную систему управления доступом на основе пароля (сертификата). Пользователи, работающие на компьютерах, должны использовать экранные заставки, защищенные паролями. Таким образом, для восстановления работоспособности компьютера после режима неактивности (экранной заставки), необходимо ввести пароль. Многопользовательские системы, используемые в Компании X, должны использовать автоматический выход системы, то есть, автоматически заканчивать сеанс пользователя после определенного периода бездеятельности. В данном разделе сотрудники подразделения информационной безопасности должны ответить на следующие вопросы:

– Существует ли утвержденная система управления доступом?

– В "Инструкции о парольной защите" есть ли положение о том, чтобы пользователи использовали экранные заставки?

– Возможно ли автоматические окончание сеанса пользователя после определенного периода бездействия в многопользовательских системах?

Внешние сетевые подключения

Все входящие подключения к компьютерам Компании X из внешних сетей должны быть защищены динамическими одноразовыми паролями. Динамические пароли отличаются всякий раз, когда они используются, и поэтому не могут быть использованы повторно для получения несанкционированного доступа. При использовании компьютеров Компании X, сотрудники не могут установить подключения к внешним сетям, включая системные службы Internet, если эти подключения не были одобрены отделом защиты информации. В данном разделе сотрудники подразделения информационной безопасности должны ответить на следующие вопросы:

– Существует ли система аутентификации, основанная на применении динамических одноразовых паролей и инструкция по ее применению?

– Существует ли инструкция по работе с Интернет?

– Предусмотрен ли в ней запретна несанкционированное подключение к внешним сетям, включая системные службы Internet.

Изменения в топологии сети

За исключением чрезвычайных ситуаций, все изменения в компьютерных сетях Компании X должны быть зарегистрированы с помощью предварительного запроса на производство работ, и заранее одобрены отделом информационных технологий. Все критические изменения сетей Компании X должны быть сделаны только людьми, уполномоченными отделом информационных технологий.

Данный раздел должен опираться на "Инструкцию о порядке внесения изменений в компьютерные сети", одобренную отделом ИТ. Удаленная работа По усмотрению руководства, некоторые квалифицированные сотрудники могут выполнять часть их работы дома. Длительное разрешение на удаленную работу частично зависит от согласия с правилами политики информационной безопасности и соответствующих стандартов. Периодическая проверка электронной почты, в дороге или из дома не считается удаленной работой, но требует от сотрудников следования многим из тех же предосторожностей защиты.

Доступ к Internet

Сотрудники, которым предоставлен доступ к

Вопросы, рассматриваемые в политике безопасности организации

Internet, должны использовать его для выполнения работ, однако этот доступ может быть прекращен в любое время на усмотрение соответствующего руководства. Доступ к Internet должен проверяться для того, чтобы гарантировать, что сотрудники не используют его в неслужебных целях, и гарантировать, что они руководствуются политикой безопасности. Сотрудники должны проявлять особую осторожность для того, чтобы гарантировать, что они не представляют Компанию X на группах обсуждения Internet и на других общественных форумах, если они предварительно не получили на это разрешение высшего исполнительного руководства. Вся информация, полученная из Internet, нуждается в проверке из надежных источников. Сотрудники не должны размещать материалы Компании X в любой публично-доступной компьютерной системе типа Internet, если размещение материалов не было одобрено Владельцем информации и начальником отдела информационных технологий. Конфиденциальную информацию, включая пароли и номера кредитных карточек, нельзя послать через Internet, если эта информация не зашифрована.

Порядок работы с электронной почтой

Каждому сотруднику Компании X, использующему для работы компьютер, предоставляется адрес электронной почты Internet и связанные с этим привилегии. Личный адрес электронной почты Internet или любой другой адрес электронной почты не должны использоваться для бизнеса Компании X, если сотрудник не получил одобрение руководства. Незапрашиваемые рассылки электронной почты клиентам запрещены. Весь персонал Компании X должен воздержаться от посылки номеров кредитных карточек, паролей или другой конфиденциальной информации. Весь штат Компании X должен использовать стандартную подпись электронной почты, которая включает полное наименование должности, название компании, адрес компании, и служебный номер телефона. Пользователи не должны хранить важные сообщения в своем входном почтовом ящике электронной почты.

Защита от вирусов

Все пользователи персональных компьютеров должны использовать актуальные версии одобренного антивирусного ПО. Пользователи не должны прервать автоматические программные процессы модификации антивирусного ПО. Антивирусное ПО должно использоваться для проверки программного обеспечения и файлов данных, полученных от третьих лиц или других подразделений Компании X. Эта проверка должна выполняться прежде чем будут открыты новые файлы данных и до запуска нового программного обеспечения. Сотрудники не должны иметь возможность обойти или выключить антивирусное ПО, чтобы предотвратить проникновение компьютерных вирусов. Приложением к данному пункту Политики безопасности должна служить "Инструкция по антивирусной защите", с которой пользователи ознакамливаются под роспись (в части касающейся).

Действия в случае подозрения на заражение вирусом

Если сотрудник подозревает заражение компьютерным вирусом, он должно немедленно прекратить использовать компьютер и позвонить в отдел защиты информации. Гибкие диски и другие магнитные носители данных, использовавшиеся при работе с зараженным компьютером не должны использоваться ни с каким другим компьютером до успешного уничтожения вируса. Инфицированный компьютер должен также быть немедленно отключен от внутренних сетей. Пользователи не должны пытаться лечить вирусы самостоятельно. Квалифицированный персонал Компании X или внешние консультанты должна завершить эту задачу способом, который минимизирует возможное разрушение данных и время простоя.

Резервное копирование

Все инсталляционные копии программного обеспечения, используемого на персональных компьютерах должно храниться в безопасном месте в виде архива лицензионного ПО. Эти главные копии не должны использоваться в повседневной работе, но должны быть зарезервированы для восстановления в случае компьютерного заражения вирусом, сбоев жесткого диска, и других проблем.

Пользователи должны регулярно копировать информацию, хранящуюся на их ПК, или принятая политика должна гарантировать, что кто-то сделает это вместо них. Для серверов и систем связи, системный администратор отвечает за совершение периодического резервирования. Все резервные копии, содержащие критическую или конфиденциальную информацию должны быть сохранены в утвержденном месте вне серверной.

Источники программного обеспечения

Компьютеры и сети не должна использовать ПО, которое исходит из посторонних источников, кроме других отделов Компании X, или доверенных поставщиков программного обеспечения. ПО, загруженное из Internet, бесплатное ПО, и прочее ПО из недоваренных источников не может использоваться, если оно не было подвергнуто строгой проверке и не одобрено отделом информационной безопасности. Необходимым условием использования эталонного программного обеспечения является получение его от производителя и последующее хранение с использованием созданных производителем контрольных сумм эталонных образцов. Так, например, поступает компания Microsoft, которая предоставляет вместе с каждым патчем его контрольную сумму. Это значительно облегчает проверку на отсутствие незаконных модификаций эталонного ПО и позволяет избежать установки ОС, заранее зараженной троянскими и шпионскими программами, ведь в таком слу-

Вопросы, рассматриваемые в политике безопасности организации

чае контрольные суммы файлов не будут совпадать с эталонными. Ведь общеизвестно, что сайты, содержащие дистрибутивы ОС FreeBSD, Linuxвзламывались хакерами неоднократно, после чего там размещалась модифицированная ОС троянскими и шпионскими закладками. Таким образом, можно констатировать переход хакеров от простого проникновения к масштабной стратегической работе в сети. Наличие же контрольных сумм эталонных дистрибутивов позволит вам избежать их подмены модифицированными образцами.

Письменные спецификации ПО

Все ПО, разработанное внутренним персоналом, должны иметь формальную письменную спецификацию. Спецификация должна быть частью соглашения междуВладельцем информации и разработчиком. Макросы в электронных таблицах и документах обработки текстов не считаются в данном разделе программным обеспечением.

Одобрение отдела защиты информации

Прикладное ПО, перед вводом в эксплуатацию должно получить письменное одобрение отдела информационной безопасности Данный раздел политики безопасности должен ссылаться на “”Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированных рабочих мест (АРМ) АС”. Эта инструкция призвана регламентировать функции и взаимодействия подразделений организации по обеспечению безопасностипри проведении модификаций и обслуживании программного обеспечения и технических средств АС, и должна содержать следующие положения. Все изменения конфигурации технических и программных средствзащищенных рабочих станций и серверов (различныхуровней защищенности)необходимо производить только на основании заявок начальников структурных подразделений организации либо заявок начальника службы информационных технологий, согласованных с руководителем службы (начальником отдела)защиты информации (ЗИ). Право внесения изменений вконфигурацию аппаратно-программныхсредств защищенныхрабочих станций и серверов АС должно быть предоставлено уполномоченным сотрудникам (должны быть утверждены соответствующими приказами) определенных подразделений:

– В отношении системныхи прикладных программных средств, а также в отношении аппаратных средств — уполномоченным сотрудникам отдела автоматизации службы ИТ; в отношении программно-аппаратных средств защиты — уполномоченным сотрудникам службы ЗИ; в отношении программно-аппаратных средств телекоммуникации — уполномоченным сотрудникам службы связи (телекоммуникации).

– Изменение конфигурации аппаратно-программныхсредств защищенныхрабочихстанций и серверовкем-либо, кроме уполномоченных сотрудников перечисленныхподразделений, должно быть ЗАПРЕЩЕНО.

– Право внесения изменений в конфигурацию аппаратно-программных средств РС АС организации, не требующих защиты, может быть предоставлено как сотрудникам отдела автоматизации (на основании заявок), так и сотрудникам подразделений, вкоторых они установлены, на основании распоряжений начальников данныхподразделений. Утверждение изменений

– Все компьютеры и системы связи, используемые для обработкиинформации должны использовать зарегистрированные процессы управления изменениями, которые используется для того чтобы гарантировать, что сделаны только утвержденные изменения.

Эта процедура управления изменениями должна использоваться для всех существенных изменений в прикладном или системном программном обеспечении, аппаратных средствах, линиях связи. Данная процедура должна быть описанав “Положении о проведении изменений в аппаратно-программной части АС”.

Неправомочное копирование

Неправомочные пользователи не должны копировать программное обеспечение, приобретенное Компанией Х, на любые носители данных, передавать (перемещать) такое программное обеспечение на другие компьютеры, или раскрывать такое программное обеспечение внешним сторонам без разрешения руководства. (Не включая обычное резервное копирование).

Защита от хищения

Все компьютерное и сетевое оборудование Компании Х должно быть физически защищено. Местные серверы локальной сети должны быть помещены в защищаемыхпомещениях, снабженных сигнализацией. Компьютеры исетевое оборудование не может быть вынесено из офиса Компании Х без разрешения соответствующего руководства.

Внешнее раскрытие систем защиты информации

Информация о мерах защиты компьютерных и сетевых систем Компании Х является конфиденциальной. Например, издательские модемные телефонные номера или другая системная информация доступа в каталогах запрещены. Раскрытие адресов электронной почты допустимо.

Права на разработанные материалы

При выполнении услуг для Компании Х, сотрудники должны предоставить Компании Х исключительные права на патенты, авторские права, изобретения, или другую интеллектуальную собственность, которую они создают или разрабатывают. Все программы и документация, созданные сотрудниками рабочими для Компании Х — собственность Компании Х. Компания Х имеет законное монопольное использова-

Вопросы, рассматриваемые в политике безопасности организации

ние содержания всех своих информационных систем. Компания X имеет право использовать эту информацию по своему усмотрению.

Право мониторинга

Компания X имеет право контролировать, осматривать или производить мониторинг информационных систем, принадлежащих компании. Эта экспертиза может иметь место с/без согласия, присутствия, или знания вовлеченных сотрудников. Информационные системы, подвергаемые такой экспертизе, включают файлы электронной почты, файлы жесткого диска персонального компьютера, файлы речевой почты, буферные файлы принтера и прочие файлы. Все исследования такого характера должны производиться после получения одобрения юридического отдела и отдела безопасности.

Поскольку компьютеры и сети Компании X предоставляются исключительно для работы, сотрудники не должны иметь никаких претензий в отношении секретности, связанной с информацией, которую они хранят или посылают с помощью этих информационных систем. Компания X сохраняет право удалить из информационных систем любой материал, который можно рассматривать как потенциальное правонарушение.

Личное использование

Информационные системы Компании X предназначены для использования только в деловых целях. Использование информационных систем Компании X для благотворительных целей, политическая кампания, материальная, религиозная работа, передача нежелательного материала, или любое другое не деловое использование запрещено.

Неподходящее поведение

Руководство Компании X резервирует право отменить системные привилегии любого пользователя в любое время. Поведение, которое неблагоприятно затрагивает способность других использовать информационные системы, или является вредным или оскорбительным в отношении других, не разрешается. Данное положение должно быть закреплено в “Пользовательском соглашении”.

Инструментальные средства безопасности

Сотрудники Компании X, если иное не определенно отделом защиты информации, не должны приобретать, обладать, торговать, или использовать аппаратные или программные инструментальные средства, которые могли бы использоваться для оценки или угроз информационной безопасности систем.

Запрещенные действия

Пользователи не должны проверять меры защиты системы связи, или пытаться ставить под угрозу компьютер, если иное не определенно и не одобрено заранее и в письменной форме начальником отдела внутреннего аудита.

Инциденты, включая неутвержденный взлом системы, восстановление пароля, расшифровку файлов, нелегальное копирование программного обеспечения, или прочие подобные неправомочные попытки угрозы мерам защиты являются незаконными, и будут рассматриваться серьезными нарушениями внутренней политики Компании X.

Сообщение о нарушении

Обо всех подозреваемых нарушениях политики безопасности, системных вторжениях, вирусных эпидемиях, и других возможных инцидентах, связанных с нарушениями безопасности информации Компании X или ее информационных систем, нужно немедленно сообщать в отдел защиты информации. Сообщения можно оставлять анонимно на автоответчике.

Заключение

В заключение хотелось бы добавить, что данный перечень вопросов, без сомнения, не является исчерпывающим и в каждом конкретном случае, несомненно, будет изменяться (дополняться). Процесс разработки политики информационной безопасности является делом не одного дня и в него должны вовлекаться все специалисты по защите информации компании. Общепринятой практикой является также использование знаний внешних консультантов, привлечение которых может дать дополнительную уверенность в том, что ничего не упущено и политика безопасности учитывает все возможные угрозы информации и использует адекватные способы противодействия им.

Обсудить

Обновления для программ

Владимир БЕЗМАЛЫЙ, vladb@windowslive.com,
специалист по обеспечению безопасности,
MVP Consumer Security,
Microsoft Security Trusted Advisor

Защита компьютера подразумевает теперь не только установку обновлений программного обеспечения компании Microsoft, но и обновление прикладных программ независимых производителей. По данным за 2011 год, в наиболее широко используемом программном обеспечении обнаружено 4733 уязвимостей. При этом к концу 2011 года неисправленными осталось 1657 изъянов. При этом распределены уязвимые места в клиентских программах по-разному, статистика представлена в таблице.

Таблица. Распределение уязвимостей в прикладных программах в 2011 году

Опасность/тип программного обеспечения	Браузеры	Офисные приложения	Мультимедийные приложения	ActiveX компоненты
Критическая	4	3	0	3
Высокая	425	127	247	83
Средняя	77	7	13	5
Низкая	88	16	10	11

Таким образом, несложно сделать вывод, что пользователям необходимо специальное программное обеспечение для установки обновлений или хотя бы отслеживания их появления, особенно в связи с многообразием установленного программного обеспечения. В Интернете можно найти множество программ, решающих подобные задачи. Я же остановлюсь только на трех продуктах.

Secunia Online Software Inspector (OSI)

Уже из названия понятно, что данное программное обеспечение работает только при подключении к Интернету. Получить доступ к нему можно, пройдя по ссылке.

Программное обеспечение Secunia Online Software Inspector — наиболее быстрый способ проверить компьютер на наличие уязвимостей для наиболее распространенных программ, таким образом, вы можете обеспечить себе минимальный уровень безопасности с помощью установки обновлений. Почему минимальный? Да потому, что проверяется всего порядка 100 программ. Перечислим возможности данного продукта:

– проверка наличия обновлений программного обеспечения от Microsoft;

– включение дополнительных функций безопасности в Sun Java;

– работает в браузере;

– не требует установки и загрузки;

– для работы необходимо наличие Java на компьютере пользователя.

Вместе с тем, для более качественной проверки специалисты компании Secunia рекомендуют владельцам домашних компьютеров использовать другое программное обеспечение от компании Secunia — Personal Software Inspector.

Рис. 1

Secunia Personal Software Inspector (PSI)

Загрузить это программное обеспечение можно по адресу. Данное программное обеспечение предназначено для домашних пользователей и предоставляется бесплатно.

PSI фактически сканирует на вашем компьютере все файлы .exe, .ocx и .dll, используя свою базу сигнатур, а затем производит автоматическое обновление найденных файлов.

Если вы нажмете кнопку Show programs, то сможете увидеть полный список отсканированных программ (рис. 1).

По умолчанию обновление программ производится вручную, но на вкладке Settings вы можете выбрать установку обновлений автоматически.

Поиск ошибок в Kaspersky Internet Security

Еще одним инструментом для поиска уязвимостей является продукт Kaspersky Internet Security. В последнее время

Обновления для программ

этот инструмент стал уже не просто антивирусом, а целым комплексом по защите компьютера. Как же в нем проводится поиск уязвимых мест? Хотя, на мой взгляд, логично было бы расположить кнопку поиска уязвимостей в разделе “Инструменты”, ведь это все же дополнительная возможность, нужная кнопка находится в меню “Проверка”.

Если вы выберете “Поиск уязвимостей”, запустится процесс анализа уязвимостей вашей операционной системы и приложений.

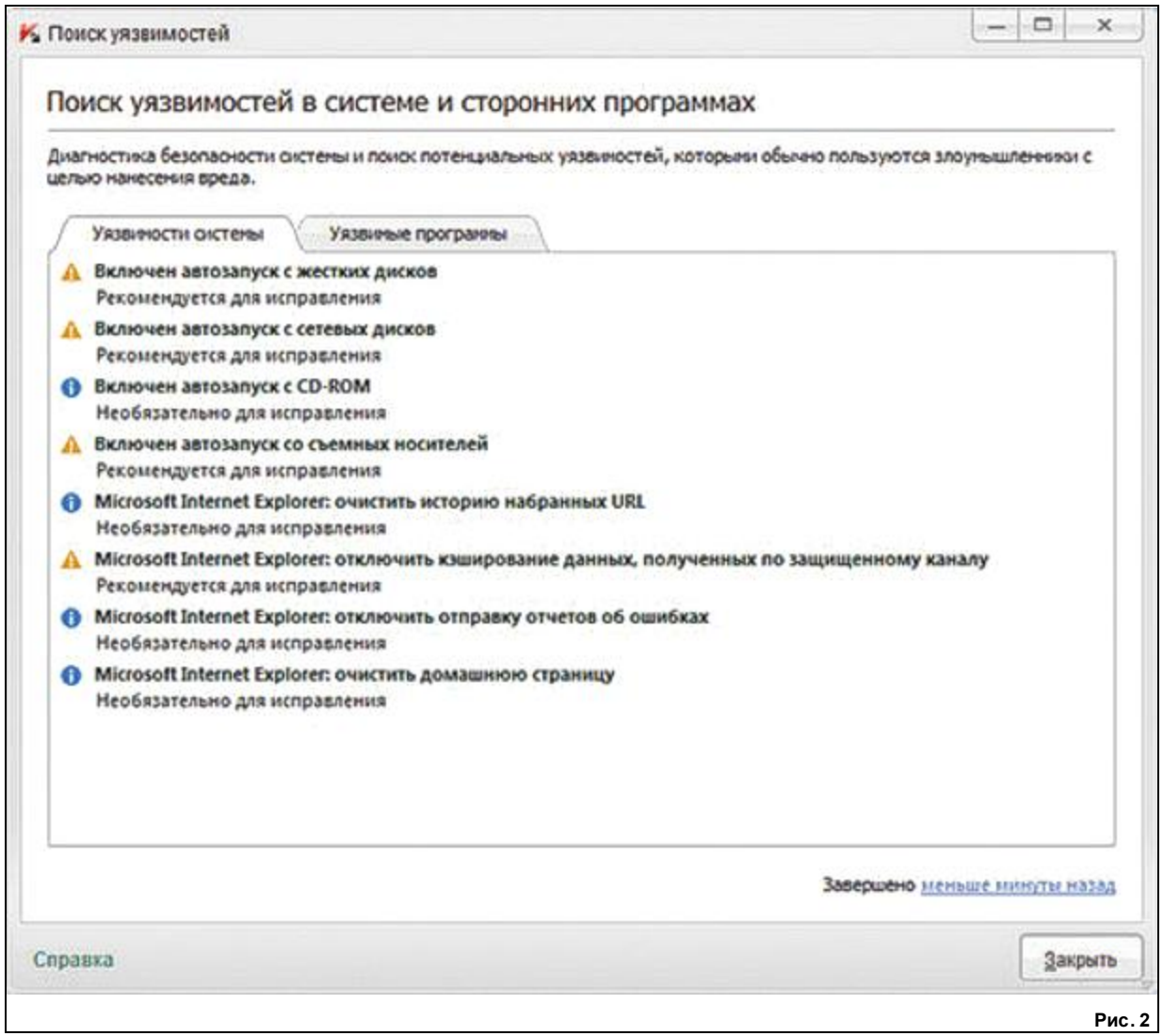


Рис. 2

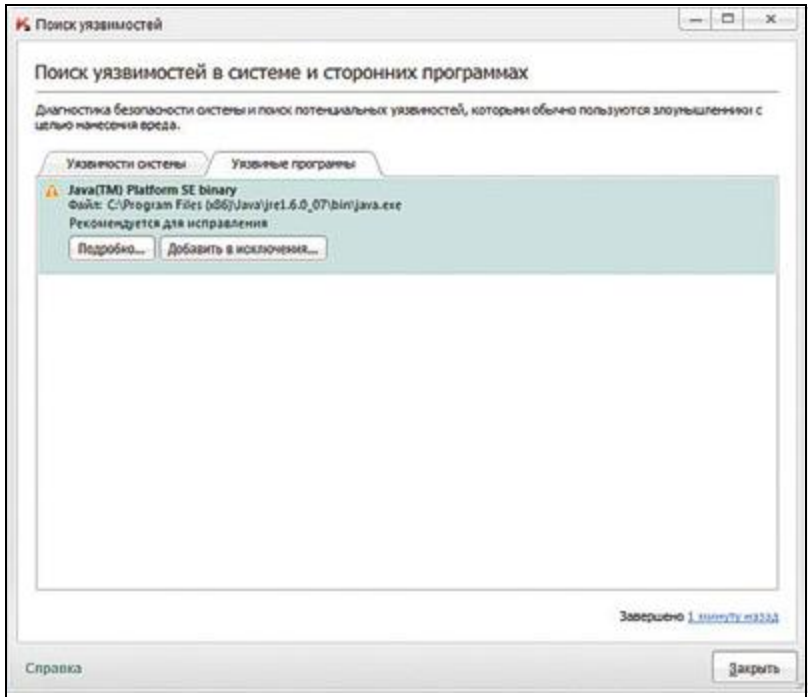


Рис. 3

Процесс поиска выполняется достаточно быстро. На моем компьютере он продолжался менее 5 минут. По окончании поиска уязвимостей вы увидите отчет, подобный представленному на рис. 2.

Как мы видим, здесь приведен список рекомендованных действий для обеспечения безопасности операционной системы и Internet Explorer, а также список уязвимых приложений. Перейдем к списку уязвимых приложений (рис. 3).

Если нажать кнопку “Подробно”, мы увидим подробную информацию об уязвимости. Изучив ее, вы сможете сделать вывод, нужно ли вам устанавливать обновление.

Итак, вы, конечно, можете сами решать, чем и как обновлять операционную систему и приложения. На мой взгляд, обновлять нужно обязательно! Могу сказать, что у меня установлены приложения PSI от Secunia и KIS, так как для процессов анализа уязвимостей, на мой взгляд, лучше использовать эти приложения параллельно.

Обсудить

ЧУМАК
З лану до столу!

SAP ERP на заводе “Чумак”

Условия, которые диктует нам тотальная глобализация, давно не являются новизной. Люди привыкли к тому, что любую необходимую вещь, включая продукты питания, можно приобрести независимо от того, где эти продукты производятся. Примером высокого качества, современного производства является компания “Чумак”— известный производитель соусов, майонезов, соков, консервированных овощей и другой пищевой продукции. Несмотря на то, что основные производственные мощности компании расположены на юге Украины (зона, именуемая “томатным поясом Европы”— регион, наиболее благоприятный для выращивания помидоров), продукты ТМ “Чумак” широко славятся и в других странах, в том числе, и в Беларуси.

Для обеспечения современного подхода к производству, поддержанию высоких мировых стандартов и требований компания старается идти в ногу с развитием инновационных технологий. В условиях необходимости повышения эффективности работы компании, решение было найдено за счет внедрения интегрированных автоматизированных процессов планирования ресурсов и управления производством. На сегодняшний день все основные производственные процессы компании “Чумак” функционируют и взаимодействуют в системе SAP ERP. Внедрение SAP позволило оптимизировать и консолидировать процессы автоматизации бухгалтерского и налогового учета, контроллинга, сбыта, учета основных средств, управления производственными мощностями и закупками, и т.д.

Компания “Инком”

Решение

Процесс реализации проекта по своей сути значительно отличался от традиционной автоматизации управления предприятием на базе решений SAP ERP. Как правило, сначала внедряется система автоматизации операций, после чего к ней подключается система бизнес-аналитики. В этом проекте руководство АО “Чумак”, согласившись с предложением системного интегратора Инком, решило начать внедрение аналитической системы одновременно с ERP-системой. Эксперимент превзошёл ожидания: в кратчайшие сроки была развёрнута система SAP BO BI (Business Object Business Intelligence), подключена к хранилищу существующей системы, и уже на начальных этапах проекта заказчик получил действующий портал корпоративной аналитической отчётности. Таким образом, инвестиции начали возвращаться, не дожидаясь старта промышленной эксплуатации всей системы.

Проект по внедрению SAP BO BI проходил в несколько

> “Роман Фисун, директор департамента консалтинга компании Инком: “Важно отметить, что заказчик проявил высокую степень зрелости и готовности к внедрению новой модели автоматизированных процессов. Как руководство, так и проектная команда АО “Чумак” продемонстрировали свою заинтересованность в реализации и успехе проекта”.”

SAP ERP на заводе “Чумак”

этапов. На первом происходило обучение специалистов завода работе со средствами аналитической системы, активное освоение полученного инструментария совместными усилиями проектных команд. На втором этапе аналитическая система была подключена к источникам статистических данных. На третьем происходило формирование системы преобразования алгоритмов получения данных в бизнес-термины. Следующий этап — формирование ряда динамических отчётов, с помощью которых можно проводить анализ в режиме реального времени. На завершающем этапе был запущен портал корпоративной отчётности: настройка планировщиков формирования информационных кубов и отчётов, их автоматическая сегментация и рассылка пользователям аналитики, настройка регламентов и прав доступа к объектам портала и сегментам данных. Таким образом, внедрение системы бизнес-аналитики позволило получить быстрый экономический эффект ещё на этапе внедрения ERP-системы — благодаря возможности оперативного принятия управленческих решений на основе анализа данных из текущей учётной системы.

> “Информационная система, успешно реализованная в АО “Чумак” с помощью решений SAP ERP и SAP Business Objects BI, стала системообразующим инструментом, поддерживающим возможности дальнейшего быстрого роста компании и обеспечивающим оперативное управление бизнесом в режиме онлайн, — отметил Максим Матяш, региональный директор SAP в Украине, Молдове и Грузии. — Завершение этого комплексного проекта в очередной раз свидетельствует о том, что украинские компании сектора среднего бизнеса всё больше связывают своё развитие с инновационными ИТ-решениями. Сегодня ИТ — не просто инструмент для поддержки управления бизнесом, но и фактор, оказывающий непосредственное влияние на перспективы роста и конкурентоспособность компаний”.

Сегодня система бизнес-аналитики формирует отчётность как на основании исторических данных, накопленных в старой системе, так и на основании данных, загружаемых из новой ERP-системы в хранилище SAP BW. Кроме того, использование облачных технологий позволило оптимизировать затраты на поддержку ИТ-инфраструктуры.

В настоящее время ключевое бизнес-подразделение компании — Trade Marketing — в полной мере использует инструментарий аналитической системы: анализирует динамику продаж, тенденции продвижения товарных групп, планирует, моделирует и анализирует результаты маркетинговых активностей, выпуска на рынок новых продуктов, освоения новых рынков. При заметном росте качества и глубины анализа ежедневные трудозатраты на формирование аналитических отчётов снизились на 60 %.

Автоматизация контроля расходов по центрам возникновения затрат заметно ускоряет этот процесс, высвободив ресурсы финансового департамента и подразделений АО “Чумак”. Автоматическая сегментация и рассылка отчётов руководителям компании и подразделений позволила избавиться от рутины и больше времени уделять задачам развития бизнеса. Большая часть отчётности теперь формируется в едином корпоративном стиле по общим стандартам и располагается в едином информационном пространстве.

> “Андрей Левчук, финансовый директор компании “Чумак”: “С самого начала задача, возложенная на проект, заключалась не просто в переносе текущих процессов компании в ERP систему. Вместе с внедрением новой системы мы хотели провести реинжиниринг процессов компании в соответствии с лучшими мировыми практиками для достижения высоких показателей эффективности производства. В результате совместными усилиями нашей команды и консультантов Инком мы успешно достигли поставленных целей”.

Соблюдение запланированных сроков позволило реализовать проект за 10 месяцев. Следующим этапом планируется внедрение систем автоматизации управления складом, а также процессов технического обслуживания и ремонта оборудования.

Обсудить

KV:\ КОМПЬЮТЕРНЫЕ ВЕСТИ
Издатель: ООО “РГ “Компьютерные Вести”
Адрес: Минск, ул. Мельникайте, 2, оф. 710.
Для писем: 220004, г.Минск, а/я 57.
Телефон/факс: (017) 203-90-10
E-mail: info@kv.by
Редакция может публиковать в порядке обсуждения материалы, отражающие точку зрения автора. За достоверность приведенной информации ответственность несут авторы.
При перепечатке материалов ссылка на “КВ” обязательна.
За достоверность рекламной информации ответственность несет рекламодатель.