ПРОТИВОДЕЙСТВИЕ ВНУТРЕННИМ ИТ-УГРОЗАМ: МИФЫ И РЕАЛЬНОСТЬ

А. Ю. Щеглов, *д. т. н., профессор*
А. А. Оголюк, *к. т. н.*
ЗАО «НПП «Информационные технологии в бизнесе»

В прошлом году было опубликовано весьма актуальное и, на наш взгляд, очень своевременное исследование компании Infowatch о внутренних ИТ-угрозах в России (www.itsec.ru от 22.11.2005). Данное исследование показало, что незащищенность информации современными системными средствами от инсайдеров, то есть пользователей, допущенных к обработке конфиденциальных данных в процессе служебной деятельности, практически по единогласному мнению специалистов, переводит проблему противодействия внутренним ИТ-угрозам (угрозам хищения информации инсайдерами) в разряд ключевых проблем защиты информации, а возможность эффективного противодействия внутренним ИТ-угрозам – в разряд доминирующих потребительских свойств средств защиты информации (СЗИ). Прошел год, ознаменовавшийся крупными скандалами вокруг событий, связанных с хищениями и раскрытием конфиденциальности персональных данных. Подводя итоги прошедшего года и анализируя изменения тенденций, специалисты Infowatch вновь провели аналогичное исследование – «Внутренние ИТ-угрозы в России 2005». Его результаты опубликованы на сайте: www. infosecurity.ru от 02.02.2006. Мы, со своей стороны, также попытались разобраться в этих вопросах, однако не в части констатации фактов (которые, кстати говоря, были предсказуемы – это следствие архитектурных особенностей построения современных системных средств), а в части выявления причин сложившейся ситуации. В результате нашего исследования были предложены общие подходы и технические решения (которые сегодня апробированы), обеспечивающие эффективное противодействие внутренним ИТ-угрозам. Материалы опубликованы на сайте компании www. npp-itb. spb. ru. В данной же статье мы попытаемся взглянуть на вновь проведенное специалистами Infowatch исследование со своих позиций, используя собственный опыт разработки средств защиты информации от внутренних ИТ-угроз.

«А ВОЗ И НЫНЕ ТАМ»

Результаты исследований, проведенных специалистами Infowatch, в части анализа критичности ИТ-угроз представлены на рис. 1–3.

Представление полученных результатов в полной мере характеризует и изменения, произошедшие за последний год. В порядке замечания отметим, что объективность исследований подтверждается специалистами Infowatch обоснованием выборки респондентов, а также снижением уровня латентности и достижением наиболее правдоподобных результатов за счет проведения опроса специалистов на анонимной основе.

Что же мы видим по результатам данных исследований? Да то, что ничего за прошедший период не изменилось. По-прежнему кража информации с целью нарушения ее конфиденциальности считается специалистами самой опасной ИТ-угрозой, а к наиболее вероятным способам хищения опять же отнесены каналы утечки данных, которыми могут воспользоваться ин-

Рис. 1

Рис. 2

Рис. 3

сайдеры. Заметим, что если подобные выводы сделаны специалистами в основном интуитивно либо на основании собственного горького опыта, то нами в предыдущих частях работы дано этому обоснование, заключающееся в том, что в основе архитектуры защиты современных универсальных ОС (в частности, ОС семейств Windows и Unix) лежит реализация принципа «полного доверия к пользователю».

Если же рассмотреть динамику изменений, произошедших за год, то можно заключить, что она незначительна. Процентные изменения, которые отражены на соответствующих рисунках, скорее могут быть отнесены к допустимой погрешности исследований, нежели служить подтверждением изменения ситуации.

СЛОВА РАСХОДЯТСЯ С ДЕЛОМ

Итак, исходя из исследований, проиллюстрированных рис. 1–3, можем сделать вывод, что необходимость противодействия внутренним ИТ-угрозам, как ключевая задача защиты информации сегодняшнего дня, специалистами осознана. Прошел целый год для принятия решений. Можно было бы предположить, что положение дел за этот срок кардинально изменится и самыми востребованными станут решения, призванные противодействовать хищению информации инсайдерами.

Результаты проведенных специалистами Infowatch исследований, иллюстрирующих популярность (или практическую востребованность) средств ИТ-безопасности, представлены на рис. 4. Что же изменилось за год? Оказывается, ничего! И что характерно, доля применения СЗИ растет, но они в большинстве своем никак не связаны с утечкой данных. Таким образом, мы видим явное противоречие: с одной стороны, понимание критичности внутренних ИТ-угроз и обеспокоенность этим специалистов, с другой – нежелание или невозможность этому противодействовать. (При этом обратим внимание на то, что сектор иных средств защиты, ориентированных, в первую очередь, на повышение стабильности функционирования информационных систем предприятия, достаточно динамично развивается.) Предполагаемые и реализуемые на практике пути противодействия утечке данных представлены на рис. 5.

Здесь опять же видим, что слова расходятся с делом. Практически единодушно заявляя о целесообразности внедрения комплексных решений на основе ИТ-технологии (другими словами, понимая единственно правильный подход к решению задачи), большинство потребителей СЗИ на практике не предпринимают никаких реальных действий по предотвращению утечки данных. Если же подобные действия и предпринимаются, то в основном они сводятся к реализации организационных мер, что, по нашему мнению, в данном случае просто бессмысленно. Интересен и тот факт, что, понимая проблемы и не предпринимая каких-либо практических шагов для их решения, потребитель не желает отказываться в пользу безопасности и от критичных сервисов, предоставляемых информационными технологиями (на рис. 5 это иллюстрирует позиция «Ограничение связи с внешними сетями»).

ЕСТЬ ЛИ СДЕРЖИВАЮЩИЕ ФАКТОРЫ?

Особый интерес вызывает то, каким образом потребители СЗИ объясняют свою пассивность в решении задач, относящихся к рассматриваемому сектору защиты информации. Выявленные специалистами Infowatch препятствия для внедрения защиты от утечки данных представлены на рис. 6. Именно эта часть исследования должна ответить на вопросы: есть ли какие-нибудь сдерживающие факторы, объясняющие сложившееся положение, и если есть, то какие?

Здесь мы видим кардинальное (практически в равных до-

Рис. 4

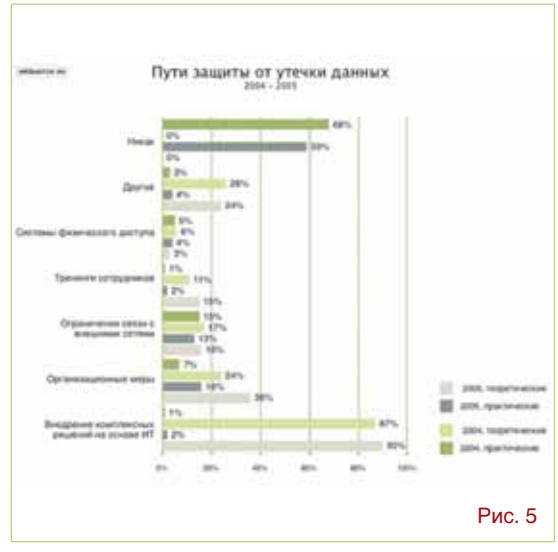

Рис. 5

Рис. 6

передача конфиденциальной информации по электронной почте и т. д. (рис. 3). Данные документы как раз и определяют требования, выполнение которых не позволит осуществить хищение данных, для этого они и предназначены. Какие же еще стандарты нужны специалистам, принявшим участие в опросе?

А вот что касается корректности данных требований (напомним, изданных еще в 1992 году) применительно к современным условиям, это уже вопрос актуальный, в котором необходимо разбираться дополнительно.

Результаты соответствующего исследования, проведенного специалистами нашей компании, применительно к решению задачи противодействия внутренним ИТ-угрозам представлены на сайте компании: www. npp-itb. spb. ru. Нами установлено, что формализованные требования, сформулированные в соответствующих нормативных документах, в полном объеме применимы в части корректного решения рассматриваемой задачи защиты конфиденциальной информации. Однако некоторые их позиции следовало бы уточнить (заметим, не изменить) с учетом архитектурных особенностей построения современных системных средств, что нами и было сделано.

Кроме того, нами были исследованы некоторые архитектурные особенности современных ОС. В результате было выявлено, что механизмами защиты, встроенными в современные ОС, данные требования (как впрочем, и ряд иных ключевых требований к защите конфиденциальной информации, не рассматриваемых в этой статье) не выполняются, чем, видимо, и объясняется их уязвимость.

Заметим, что требования, формализуемые рассмотренными выше нормативными документами, рассматривают задачу защиты информации в комплексе. Именно такой подход (это отмечают и специалисты – рис. 5) может обеспечить защиту данных, в том числе в части их возможного хищения инсайдерами. Таким образом, защита информации техническими средствами должна обеспечиваться комплексно, а не использованием отдельных частных решений и, тем более, не реализацией организационных мер.

Теперь вернемся к обозначенной специалистами и, судя по результатам исследований (рис. 6), по-прежнему актуальной проблеме отсутствия технологических решений. Здесь можем отметить, что в соответствии с нормативными документами любое средство защиты информации от несанкционированного доступа (СЗИ НСД), позиционирующееся разработчиком как обеспечивающее выполнение требований к СВТ 5-го (или выше) класса защищенности, в принципе должно гарантировать возможность эффективного противодействия внутренним ИТ-угрозам (в том числе в части хищения данных инсайдерами). Однако, как мы отмечали, некоторые требования нормативных документов требуют уточнений применительно к их использованию в современных условиях. То есть сейчас существует возможность их неоднозначного трактования как разработчиками СЗИ, так и их потребителями. Как следствие, существует и потенциальная опасность того, что какое-либо из представленных на рынке средств защиты информации от НСД (на первый взгляд, в полном объеме выполняющее требования соответствующих нормативных документов) не сможет обеспечить эффективного решения рассматриваемых в работе задач. Справедливости ради отметим, что подобные средства нам известны. Некоторые из них не то чтобы повторяют возможности встроенных в ОС механизмов защиты со всеми их недостатками, но попросту используют эти механизмы, предоставляя лишь собственный интерфейс их настройки. Здесь ведь надо понимать следующее: оставьте неперекрытым лишь один «канал» НСД (например, файловые объекты, не разделяемые системой и приложениями, буфер обмена и др.) и применение подобного СЗИ НСД будет просто бесполезным. Во избежание выбора потребителем СЗИ, не соответствующего реальным потребностям, мы предлагаем использовать результаты исследований, представленные на сайте компании: www. npp-itb. spb. ru. В частности, нами сформулированы уточняющие требования, которые мы позиционируем, как методологическую основу оценки эффективности применения СЗИ НСД для решения задачи противодействия внутренним ИТ-угрозам. При этом для того, чтобы оценить целесообразность использования того или иного средства защиты информации для решения рассматриваемых задач, потребителю достаточно убедиться, что СЗИ НСД реализует сформулированные уточняющие требования.

Будем надеяться, что ознакомление с этими материалами позволит специалистам кардинально изменить свое мнение по двум важнейшим позициям: «Отсутствие стандартов» и «Отсутствие технологических решений» (рис. 6).

И еще одно замечание. Все предлагаемые нами технические решения по противодействию внутренним ИТ-угрозам (14 из которых запатентованы) реализованы и апробированы в Комплексной системе защиты информации «Панцирь-К» для ОС Windows 2000/XP/2003 (разработка ЗАО «НПП «Информационные технологии в бизнесе», сертификат ФСТЭК № 1144 от 17.01.2006 на соответствие СВТ 5-му классу защищенности). Это позволяет нам утверждать, что эффективные технологические решения существуют.

Итак, в заключение подытожим все вышесказанное. В результате проведенного исследования мы не увидели каких-либо явных причин, препятствующих решению задачи противодействия внутренним ИТ-угрозам – хищению конфиденциальной информации инсайдерами. Это, с одной стороны, внушает некоторый оптимизм: задача может быть эффективно решена; по крайней мере, средства, позволяющие это сделать, существуют, причем они сертифицированы на соответствие требованиям информационной безопасности, которые также существуют применительно к решению данной задачи. Таким образом, формальные препятствия на пути их внедрения отсутствуют. Кроме того, существует и понимание необходимости решения этой задачи как одной из ключевых на сегодняшний день задач защиты информации. С другой стороны, это внушает и некоторые опасения, поскольку мы видим, что всё это имело место и год назад, но при этом какого-либо существенного изменения положения дел за это время не произошло.

лях) изменение ситуации по трем позициям: «Нехватка квалифицированного персонала», «Отсутствие стандартов», «Отсутствие технологических решений».

Акцентирование внимания на проблеме нехватки квалифицированного персонала является весьма отрадным. Как ни странно, но это как раз и свидетельствует о повышении профессионального уровня лиц, влияющих на принятие решения: «портрет» респондентов, принявших участие в исследовании, приведен на рис. 7.

Рис. 7

Заметим, что обеспечение информационной безопасности – это крайне сложная научно-техническая задача. Поэтому специалисты, принимающие участие в ее решении, должны обладать знаниями во многих областях (вычислительная техника, средства телекоммуникаций и т. д.), разбираться в принципах и архитектурных особенностях построения современных системных средств и приложений, иметь необходимые навыки программирования. Наивно полагать, что, обучившись навыкам администрирования какого-либо средства защиты (либо нескольких средств), человек, не имеющий хорошего базового образования в области вычислительной техники, сможет решать задачи защиты информации. Ведь даже выбор эффективного СЗИ или специализированной компании, привлекаемой для обеспечения безопасности корпоративной сети предприятия, – это уже нетривиальные задачи, требующие высокой квалификации при решении.

В порядке замечания отметим, что некоторые компании-разработчики идут «на поводу» у потребителя с его проблемами нехватки квалифицированного персонала. Однако, на наш взгляд, само утверждение, что СЗИ отличается простотой администрирования, не имеет права на существование (другое дело, что необходимо разрабатывать интерфейсы, максимально упрощающие эту задачу). Следует не упрощать СЗИ, сводя его администрирование к нажатию одной «красной кнопки» (этим можно обеспечить лишь иллюзию защиты – развитые механизмы защиты подобным образом не настроить), а повышать квалификацию лиц, обеспечивающих безопасность на предприятии. Когда информация становится товаром, эффективно противодействовать ее хищению можно, только обладая необходимой квалификацией. Что же касается тех, кому хватает иллюзии защиты, то они, скорее всего, либо отключат добавочное средство (которое априори вносит некоторое неудобство при эксплуатации информационной системы и требует вложения дополнительных средств в подготовку специалистов), либо вообще ограничатся лишь возможностью встроенных в ОС механизмов защиты.

Однако будем надеяться, что в общем случае сдерживающим фактором при решении задачи противодействия внутренним ИТ-угрозам является нежелание вкладывать дополнительные средства в защиту информации. Это подтверждают и результаты исследования по позиции «Бюджетные ограничения» (рис. 6), правда, косвенно, так как в опросе участвовали не лица, принимающие решения, а специалисты (рис. 7).

Теперь рассмотрим две, на наш взгляд, взаимосвязанные позиции: «Отсутствие стандартов» и «Отсутствие технологических решений». Вот здесь начинается самое интересное и непонятное. С одной стороны, специалисты кардинально пересмотрели свою точку зрения относительно отсутствия технологических решений, признав, что подобные решения существуют. С другой стороны, пропорционально возросла доля специалистов, отмечающих отсутствие стандартов, формализующих требования к решению задачи противодействия хищению данных инсайдерами (кстати, как увидим далее, это отголоски нехватки квалификации, что, вообще говоря, и не скрывают респонденты).

Невольно возникает вопрос: о каких решениях, о которых осведомлены специалисты, участвовавшие в опросе, тогда идет речь. Естественен и другой вопрос: неужели противодействие хищению данных – это столь новая, неожиданно возникшая задача? Неужели лишь появление проблемы инсайдеров заставило нас, наконец, задуматься о возможном хищении информации и, как следствие, о необходимости разработки соответствующих стандартов?

Для ответа на эти вопросы обратимся к двум ныне действующим основополагающим нормативным документам в области защиты информации (трудно предположить, что лица, выступающие в роли специалистов в области защиты информации, не ознакомились с этими документами). Это:

- «Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации»;
- «Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации».

Заметим, что первый из них формализует требования к корректности реализации механизмов защиты и используется при сертификации СЗИ, второй – устанавливает требования к достаточности набора механизмов защиты применительно к условиям эксплуатации защищаемого объекта и используется при аттестации объектов информатизации. Таким образом, в совокупности эти документы формализуют и то, какой набор механизмов защиты должен иметь место на защищаемом вычислительном средстве, и то, какими функциями должен обладать каждый из этих механизмов (уточним, что при защите конфиденциальной информации речь идет о требованиях к СВТ 5-го класса защищенности и АС класса 1Г).

Назначение этих документов определяется их названием (здесь двух мнений быть не может) – это защита от несанкционированного доступа к информации. Под НСД понимается доступ в обход заданной разграничительной политики, то есть в обход того, что не разрешается. В нашем случае это запрещенная запись конфиденциальной информации на мобильные накопители, запрещенная