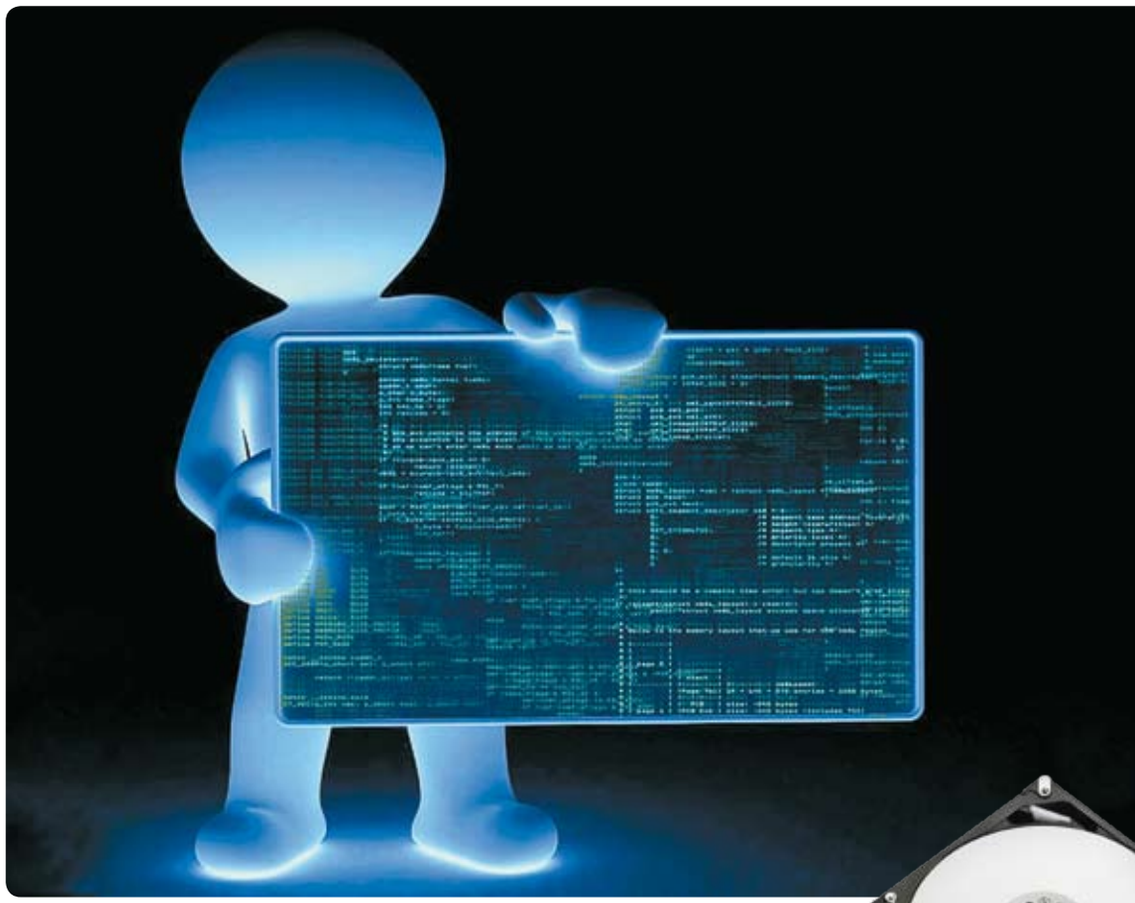
Тема безопасности востребована, и для удовлетворения спроса предлагается большое количество книг и статей, подробно раскрывающих отдельные вопросы. При этом те, кто впервые столкнулся с решением вопросов безопасности, зачастую за деревьями не видят леса, не понимая общей постановки задачи. В итоге они сосредоточиваются на решении какой-либо второстепенной проблемы, не решая при этом первостепенной, пребывая в заблуждении, что обеспечили необходимый уровень безопасности.

Что же означает обеспечение необходимого уровня безопасности?



«Бумажная безопасность»

Владимир НИКОНОВ,
преподаватель учебного центра «Информзащита»

По сути, это решение вопроса разграничения доступа в помещения, к рабочим местам и данным, которые обрабатываются в различных информационных и платежных системах.

У нас есть немало средств разграничения доступа: аппаратные и программные, есть средства, встроенные в операционную систему разработчиками компании Microsoft, а есть средства, предлагаемые другими разработчиками.

Как решается вопрос разграничения доступа в помещения?

Предварительно происходит разделение посетителей на доверенных и не доверенных, т. е. тех, кто по нашему решению имеет право доступа в помещение, и тех, кто не имеет. Готовятся списки доступа, обычно это докладные записки или приказы о допуске, но возможно и занесение учетных записей в таблицы, которые используются применяемыми нами системами доступа. Технически доступ разграничивается с помощью замков кодовых или электронных, к считывателям которых сотрудники прикладывают свои карты доступа, в особых случаях используются считыватели для отпечатков пальцев или сканирование роговицы глаза.

Как решается разграничение доступа к рабочему месту, например, к компьютеру?

Предварительно должен быть решен вопрос с должностными обязанностями сотрудников. Необходимо определиться с тем, какие сотрудники могут использовать данное рабочее место, разделить их на группы по предоставленным им полномочиям и решаемым ими задачам. После этого можно воспользоваться встроенными средствами операционной системы, такими как локальные или групповые политики. Используя эти средства, создаем учетные записи пользователей, объединяем их в группы и указываем разрешения на выполнение определенных задач на данном рабочем месте. Возможно разграничение доступа с помощью программно-аппаратных средств.

Как решается разграничение доступа к данным?

Первоначально нужно определиться, с какими данными может работать пользователь или группа пользователей, основываясь на должностных обязанностях сотрудников или на решениях о предоставлении доступа пользователям к используемым системам обработки данных. После этого предоставляем доступ доверенным пользователям путем создания для них учетных записей. Возможно, это данные, которые хранятся и используются одним пользователем компьютера, или же те, к которым предоставляется доступ группе пользователей, а может, это данные, с которыми работает группа пользователей на разных рабочих местах. В зависимости от того, как происходит доступ к данным, можно использовать средства разграничения доступа разных разработчиков. Это могут быть и встроенные средства операционной системы Microsoft, или службы управления доступом Rights Management Services,

созданные разработчиками Microsoft. Могут быть средства, созданные другими разработчиками. Эти средства обладают большими возможностями по разграничению доступа, с их помощью можно ограничить доступ как к данным на компьютере, так и к данным на отдельных устройствах, подключенных к компьютеру. Можно также ограничить доступ к отдельным портам, кроме того, отслеживать все события, связанные с нарушением безопасности, и своевременно принимать меры.

В целом имеется большой выбор средств разграничения доступа для решения наших задач, но прежде чем их приобрести, установить и использовать, необходимо детально разобраться, к каким данным будет ограничен доступ, кто из пользователей будет получать доступ и кто будет уполномочен принимать решения о доступе и следить за выполнением принятых решений. Необходимо также знать и законодательную основу защиты данных и разграничения доступа.

Общие понятия определяет Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

Статья 16. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Правительство Российской Федерации принимает правовые меры, осуществляя государственное регулирование отношений в сфере защиты информации путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Подразделения безопасности или ответственные сотрудники решают задачу подготовки и принятия необходимых организационных мер.

Только выполнив всю подготовительную работу, можно приступать к вопросу о технических мерах.

Не всегда у тех, кто впервые решает вопросы безопасности, есть понимание, какие шаги необходимо будет сделать.

Какие средства защиты обеспечивают наибольший уровень безопасности?

Желание обеспечить самый высокий уровень безопасности понятно, но с этим вопросом зачастую связаны неверные представления о первостепенном значении выбора средств защиты. Дело в том, что те, кто не имеет опыта в решении вопросов безопасности, нередко заблуждаются, считая, что все, что им нужно, — это приобрести и установить самое мощное из имеющихся средств. Это вовсе не так, на самом деле выбор используемых средств имеет второстепенное значение. Сначала надо определиться с тем, что мы будем защищать, от кого защищать, кто именно будет это делать, как научить этому и как добиться правильного выполнения. Для этого нужна большая подготовительная работа, которая предполагает создание положений, руководств и инструкций, назначение ответственных и проведение их обучения. Без выполнения этой бумажной работы любые самые развитые средства обеспечения безопасности бесполезны.

«Бумажная безопасность» — эта фраза дает очень точное представление об образе мыслей тех, кто недавно стал заниматься решением вопросов обеспечения безопасности. Они придают первостепенное значение выбору средств защиты и не решают основную задачу. Неверное понимание не только мешает работе, поскольку включается внутреннее противодействие выполнению того, что им представляется неправильным, но и в конечном итоге не приводит к решению вопроса создания необходимого уровня безопасности. Все когда-либо через это проходили и не только при решении вопросов безопасности, и чтобы все-таки учиться на чужих ошибках, расскажу на примере, как происходит внедрение средств защиты.

Описываемые ниже события происходили в одном хорошо всем известном крупном учреждении.

Мы работали в подразделении безопасности не первый год, и у нас уже был опыт внедрения и использования различных программных и технических средств безопасности.

Для обеспечения более высокого уровня безопасности при работе с документами было закуплено развитое программное средство контроля доступа к данным и установлено на нескольких рабочих местах. Мы узнали об этом, когда нас назначили ответственными и поставили задачу организовать работу с этим средством. Начав ознакомление с описания программного продукта, мы были поражены его возможностями. Выбором настроек можно было осуществлять контроль доступа пользователей или групп пользователей к документам и данным, использование ими любых внешних носителей, дисководов, принтеров и других типов устройств. Можно было контролировать время доступа пользователей, осуществлять контроль за передаваемыми данными, проводить анализ связанных с безопасностью событий, происходящих на рабочих местах пользователей. И все это можно было делать удаленно с компьютера администратора системы.

Таким образом, мы получили средство с большими возможностями, оно было готово к работе, и от нас хотели получить первый отчет по итогам контроля. И всего-то нужно было указать в настройках, какие события необходимо контролировать, а здесь как раз у нас не было ясности. Предварительная работа не была выполнена, и мы не знали, на каких рабочих местах хранятся те или иные данные, как обрабатываются и как передаются, что из этих данных нужно защищать, кто из сотрудников имеет право работать с защищаемыми данными.

Чтобы получить эти сведения, мы направили в подразделения запросы с предложением указать, сколько имеется компьютеров, какие установлены на них программные средства, какие данные и кем обрабатываются и передаются, какие используются дисководы, устройства ввода-вывода и внешние носители. Мы были уверены, что быстро получим все необходимые сведения, поскольку учет компьютеров и других технических средств велся в бухгалтерии. Кроме того, свой учет вело подразделение, которое занималось техническим обслуживанием, еще одно подразделение вело учет пользователей, имеющих право доступа к сетевым ресурсам. Но когда мы получили ответы на запросы, то оказалось, что данные учета сильно расходятся. Чтобы согласовать их, мы направляли уточняющие запросы, но с каждым полученным ответом расхождение только увеличивалось. Мы стали разбираться, и оказалось, что те, кому было поручено вести учет, не понимали его важности и считали обузой, мешающей выполнению их основной работы. Поэтому учет велся от случая к случаю, изменения вносить не спешили, а данные не сверяли.

Через месяц стало ясно, что мы теряем время и нам нужно самим начинать все с чистого листа. Согласовав с подразделениями проведение работ по сбору данных, мы последовательно обошли все помещения и пересчитали компьютеры, определили их параметры, какое количество портов и дисководов, какие устройства ввода-вывода, являются компьютеры сетевыми или автономными, что за операционная система и программы на них установлены.

Через пару месяцев мы получили общую картину, общее число компьютеров оказалось больше, чем проходило по всем учетам. На некоторых были установлены программные продукты, которые были задействованы для решения какой-либо одной редко выполняемой задачи.

Мы собрали общие сведения о компьютерах, но у нас не был решен вопрос о том, где и какие данные обрабатываются, к каким данным нужно контролировать доступ и кто из сотрудников с ними может работать. Если вы думаете, что это просто, попробуйте спросить сотрудника, решение каких задач входит в его обязанности. Пришлось собирать сведения по частям. Перечень должностных обязанностей — у руководителя подразделения, доступ к ресурсам — у сетевого администратора, порядок прохождения и обработки данных — у администраторов используемых систем для работы с данными, использование средств защиты данных — у администратора безопасности. Нужно было разобраться, как данные попадают на рабочее место, как дальше передаются, использование каких портов и устройств нужно разрешить, а каких запретить, без этих сведений настроить средство контроля было невозможно. Есть известный способ решения: если не ясно, что нужно разрешить, то надо все запретить, а при обращении пользователей каждый вопрос о снятии запрета решать отдельно.

Мы на это не пошли, чтобы не остановить работу всех подразделений, но решили опробовать удаленное управление доступом и выбрали неиспользуемые параллельные порты (LPT). Раньше эти порты использовали принтеры, но у нас давно все принтеры подключались через USB-порт. Прямо со своего администраторского компьютера отключили LPT-порты в бухгалтерии. Оказалось, что хотя принтеры и подключаются через USB-порт, но программное обеспечение компьютера считает, что данные передаются через LPT-порт. Поэтому при отключении LPT-портов все принтеры бухгалтерии остановились. Сотрудники, не понимая в чем дело, вызвали системного администратора, который переустановил им драйверы. А мы в это время решили, что зря начали с бесполезных LPT-портов, и снова их включили. Принтеры в бухгалтерии заработали, и системный администратор с чувством выполненного долга ушел.

Этот опыт показал, что можно легко управлять доступом, но нужно предварительно опробовать действие настроек на одном из рабочих мест, где не столь значительны последствия нарушения рабочего ритма. И только после этого ограничивать доступ на всех остальных рабочих местах, предварительно согласовав с руководителями подразделений перечни используемых сотрудниками портов и устройств, а также списки пользователей.

Через полгода основная часть подготовительной работы была выполнена и сведения о работе с данными на рабочих местах собраны, мы согласовали перечни устройств и списки пользователей, имеющих право работать с данными. После этого, проверив предварительно действие настроек по ограничению доступа на выделенном рабочем месте, стали устанавливать ограничения и контроль доступа на других рабочих местах, а через месяц получили первый отчет по итогам контроля.

В итоге мы еще раз убедились, что без подготовительной работы невозможно использование средств защиты и что «бумажная безопасность» имеет первостепенное значение по отношению к другим задачам.