Что нужно знать руководителю об информационной безопасности

Наталья Храмцовская,
ведущий эксперт по управлению документацией компании «Электронные офисные системы», член Гильдии управляющих документацией, член ARMA International, Москва

КАК И В ОТНОШЕНИИ МНОГИХ ДРУГИХ АСПЕКТОВ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ, РУКОВОДИТЕЛЬ НЕ ДОЛЖЕН БЫТЬ ЭКСПЕРТОМ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ГЛАВНОЕ, ЧТО ЕМУ НУЖНО, — ЭТО ПРАВИЛЬНО ПРЕДСТАВЛЯТЬ СЕБЕ ВАЖНОСТЬ И ОТВЕТСТВЕННОСТЬ ДАННОГО НАПРАВЛЕНИЯ, ЕГО ВЗАИМОСВЯЗЬ И ВЗАИМОЗАВИСИМОСТЬ С ДРУГИМИ ВИДАМИ ДЕЯТЕЛЬНОСТИ, С ТЕМ, ЧТОБЫ ВЫДЕЛИТЬ АДЕКВАТНЫЕ ЛЮДСКИЕ И МАТЕРИАЛЬНЫЕ РЕСУРСЫ, ПОСТАВИТЬ ЗАДАЧИ И НАЛАДИТЬ КОНТРОЛЬ ИСПОЛНЕНИЯ. В ТЕКУЩЕЙ СЛОЖНОЙ ЭКОНОМИЧЕСКОЙ СИТУАЦИИ ЗАЩИТА ИНФОРМАЦИОННЫХ РЕСУРСОВ ОРГАНИЗАЦИИ ОТ РАЗЛИЧНОГО ВИДА УГРОЗ СТАНОВИТСЯ ВСЕ БОЛЕЕ АКТУАЛЬНОЙ.

Ключевые слова: информация, документ, документооборот, руководитель организации, информационная безопасность, информационные ресурсы, политика безопасности.

Почему необходимо защищать информацию?

Информация и поддерживающие ее информационные системы и сети являются ценными производственными ресурсами организации. Их доступность, целостность и конфиденциальность необходимы для нормальной деятельности организации.

ПРИМЕР 1

Из «Стандарта Банка России...»

5.9.... Собственник должен знать, что он должен защищать. Собственник должен знать и уметь выделять (идентифицировать) наиболее важный для его бизнеса информационный актив (ресурс) [1].

Все чаще и чаще информационные ресурсы организаций становятся как объектом умышленных преступных действий, так и неумышленного воздействия, связанного с природными и техногенными факторами. Информационным системам и сетям угрожают такие опасности, как мошенничество, шпионаж, саботаж, вандализм, пожар, наводнение, отключение электроэнер-

СЛОВАРЬ КАДРОВОГО ДЕЛОПРОИЗВОДСТВА

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННАЯ — 1) комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с ее доступностью для всех авторизованных пользователей; 2) показатель, отражающий статус защищенности информационной системы. Отдельные сферы деятельности (системы государственного управления, банки, информационные сети и т.п.) требуют специальных мер обеспечения информационной безопасности и предъявляют особые требования к надежности функционирования в соответствии с характером и важностью решаемых задач. Достигается за счет реализации комплекса мероприятий и средств защиты, основанных на внутрифирменной политике безопасности и анализе рисков, допустимых для данной компании в конкретный период времени.

гии и многие другие. Все более распространенными, опасными и изощренными становятся такие виды угроз, как вирусы и хакерские атаки. Одновременно растет зависимость организаций от информационных систем и сервисов как компьютерных, так и «бумажных», и, как следствие, соответственно увеличивается потенциальный ущерб в случае неприятностей.

Распространение вычислительных сетей предоставляет новые возможности для несанкционированного доступа к компьютерным системам, а переход на распределенные вычислительные системы уменьшает возможности централизованного контроля. В то же время отказ во многих организациях от жесткой вертикальной структуры, широкомасштабное делегирование полномочий, распределенная организационная структура крупных объединений и холдингов усложняют поддержание режима информационной безопасности (ИБ) в системах традиционного «бумажного» документооборота.

Сейчас в организации существуют два основных информационных потока: электронный и бумажный. При разработке системы информационной безопасности нужно учитывать их особенности и защищать информации независимо от того, в какой информационной системе и в каком потоке она находится.

Информационная безопасность и ее иллюзии

Информация представляет собой ценный деловой актив организации, и, следовательно, должна быть надлежащим образом защищена. Информационная безопасность означает защиту информации от разнообразных опасностей, с тем, чтобы обеспечить бесперебойную работу, минимизировать возможный ущерб и максимизировать деловые возможности и отдачу от инвестиций.

Информация существует в различных формах. Она может быть распечатана или записана на бумаге, может храниться в электронной форме или в памяти сотрудников; ее можно пересылать как по обычной почте, так и при помощи современных средств связи. Информацию можно показать, используя изображения на пленке, или же высказать в беседе. Какую бы форму информация ни принимала, какие бы средства ни использовались для ее хранения и распространения, — она всегда должна быть надежно защищена.

Информационная безопасность подразумевает:

- обеспечение конфиденциальности — информация доступна только тем, кто имеет на то соответствующее право;
- обеспечение целостности — защищается точность и полнота информации, а также методов ее обработки;
- доступность — гарантируется, что авторизованные пользователи, когда нужно, имеют возможность получить доступ к информации.

Для достижения информационной безопасности используется ряд методов и средств, включая разработку и внедрение внутренних нормативных документов, инструкций и правил, создание специальных структурных подразделений, отвечающих за координацию этой работы, а также использование специального программного обеспечения.

Иллюзия 1: информационная безопасность = компьютерной безопасности. Исторически понятие «информационная безопасность» возникло как расширенное толкование деятельности, связанной с обеспечением компьютерной безопасности. По-прежнему для большинства сотрудников (не говоря уже о специалистах службы информационных технологий) эти два термина равнозначны.

Для современного руководителя отождествление информационной безопасности с компьютерной безопасностью — ошибка, чреватая серьезными последствиями.

Например, все бумажные документы организации — тоже информация, безопасность которой традиционно обеспечивается службой документационного обеспечения управления (ДОУ), в состав которой могут входить секретариат, канцелярия, общий отдел, архив и другие подразделения. В России пока что бумажным документам доверяют больше, чем электронным, для которых еще не создана полноценная законодательно-нормативная база и не сложилась общепринятая практика, — поэтому важная информация, как правило, фиксируется на бумаге. Как следствие, защита одних только электронных документов, серверов, сетей и т.д. не может обеспечить подлинной информационной безопасности и приводит к малоэффективному расходованию ресурсов.

Более того, для обеспечения информационной безопасности необходима согласованная работа всех заинтересованных служб: IT-службы, ДОУ, кадровой службы, службы безопасности, юридической службы, службы внутреннего контроля и других. Все виды информации, на всех видах носителей должны защищаться в соответствии с едиными принципами, регламентирующими правила доступа к информации, правила создания/захвата, хранения, экспертизы ценности и уничтожения информации.

Иллюзия 2: информационная безопасность — это только борьба с преступниками. Еще одна иллюзия, широко распространенная среди руководителей организаций, — это представление об информационной безопасности главным образом как о борьбе с различного рода преступниками. На самом деле программа информационной безопасности решает гораздо более обширный круг задач:

- защита информационных ресурсов организации от иных видов угрозы, таких как природные явления (наводнение, пожар) или же техногенные катастрофы (отключение электроэнергии);
- обеспечение долговременной сохранности целостных и аутентичных информации и документов, подлежащих длительному и постоянному хранению, — что является непростой и до конца пока еще не решенной задачей в отношении электронных документов (в связи с физическим и моральным устареванием носителей информации, оборудования, форматов и программного обеспечения);
- защита юридических, имущественных и иных прав организации, ее сотрудников и клиентов путем соблюдения установленных норм и правил делопроизводства и документооборота. Сюда входят своевременное создание необходимых документов, хранение в течение установленного срока, своевременное уничтожение информации в строгом соответствии с законодательством, а также защита персональной информации и информации, являющейся интеллектуальной собственностью;
- обеспечение сохранности и быстрого доступа к информации, которая необходима для быстрого восстановления деятельности организации в случае непредвиденных обстоятельств. Этот вид деятельности требует защиты иного круга информационных ресурсов, часто — на таких носителях, для использования которых не требуются технические средства.

Защита одних только электронных документов, серверов и сетей не может обеспечить подлинной информационной безопасности и приводит к малоэффективному расходованию ресурсов.

«Семь нянек» информационной безопасности

В организациях существует несколько видов информационных ресурсов, каждый из которых имеет свои особенности:

1. Электронные документы и информация хранятся в компьютерных системах и сетях. Обычно за сохранность этой информации несет ответственность служба информационных

технологий. IT-служба обеспечивает бесперебойную работу всех систем, регулярное резервирование информации и т.д.;

2. За бумажные документы главным образом отвечает служба документационного обеспечения управления. Документы хранятся в защищенных помещениях или в закрытых шкафах. Ведется регистрация и учет документов как созданных, так и полученных. Часть бумажных документов, в том числе конфиденциальных и содержащих персональные данные, контролируется другими службами организации (юридической, кадровой и т.д.). В последнее время все чаще используется аутсорсинг — передача документов на внеофисное хранение сторонней коммерческой организации. Работа с бумажными документами и информацией, которая в них содержится, как правило, хорошо регламентирована и отлажена. Соблюдение правил работы с документами позволяет обеспечить информационную безопасность организации на протяжении всего жизненного цикла документов и информации, от момента создания или получения до момента уничтожения в связи с истечением сроков хранения;

Часто наиболее ценная и важная информация хранится в головах сотрудников. Американцы говорят, что 65% информации ежедневно вечером покидает офис фирмы и может утром не вернуться, — или, хуже того, перебежать к конкурентам.

3. Может быть, наиболее ценная и важная информация хранится в головах сотрудников. Как говорят американцы, руководитель организации всегда должен помнить, что 65% информации ежедневно вечером покидает офис фирмы и может утром не вернуться, — или, хуже того, перебежать к конкурентам. О защите этого ресурса обычно не задумываются — до тех пор, пока не уволится или не заболеет ключевой сотрудник, без которого работа встает. Формальную ответственность за этот ресурс не несет никто, но в первую очередь его защищенность зависит от действий высшего руководства организации, кадровой службы и службы безопасности.

В итоге у информационной безопасности оказывается «семь нянек» — администрация, служба ДОУ, служба безопасности, отдел кадров, ИТ, юридический отдел, деловые подразделения. Каждая из этих «нянек» занимается только «своими» вопросами, не согласовывая и не координируя свою деятельность с деятельностью других служб. Эта разобщенность приводит к появлению колоссальных дыр в общей системе информационной безопасности, — например, из-за возникновения «нестыковок» в предоставлении прав доступа к информации и документам на различных носителях.

Самое слабое звено в обеспечении информационной безопасности

Уязвимость любой системы оценивается по наиболее слабому звену. Накопленный опыт недвусмысленно показал, что ключевая проблема в обеспечении безопасности — проблема кадровая.

ПРИМЕР

Из исследовательского отчета фирмы «Эрнст и Янг»

6. Люди остаются самым слабым звеном в обеспечении информационной безопасности.

Инвестиции в технологии немногого стоят, если не обучать сотрудников тому, что и как делать. Этот факт еще раз подтверждают несколько недавних инцидентов, получивших большой общественный резонанс, при расследовании которых в конечном итоге выяснилось, что их причиной стали не технические уязвимости, а человеческие ошибки.

На технологии делается настолько большой упор, что о «человеческой» составляющей информационной безопасности часто забывают. Результаты опроса 2008 года подтверждают, что во многих компаниях эта проблема остается нерешенной [6].

Статистика свидетельствует о том, что большинство удачных атак либо идут изнутри организации, либо при содействии кого-то из сотрудников. При помощи одних только технических и программных средств надежную защиту обеспечить очень трудно,

тем более, что сейчас в распоряжении злоумышленника может находиться арсенал средств, продаваемых в магазинах по вполне умеренным ценам, которому лет двадцать-тридцать назад позавидовали бы ведущие разведки мира, а на каждую новинку в области защиты быстро находится «противоядие».

ПРИМЕР

Из «Стандарта Банка России...»

5.4. Наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является нецелевое использование предоставленного контроля над информационными активами, а также сокрытие следов своей деятельности. Внешний злоумышленник, скорее, да, чем нет, может иметь сообщника (ов) внутри организации [1].

Меры, необходимые для уменьшения угрозы со стороны персонала, общеизвестны и записаны во все стандарты и руководства (другое дело, что реализовать их на практике не так-то легко):

- все принимаемые на работу сотрудники должны проверяться;
- следует поощрять бдительность на рабочих местах и предусмотреть способы, при помощи которых сотрудники могли бы сообщать о подозрительной деятельности.

Интересные данные приведены в опубликованном в августе 2004 года совместном исследовании, проведенном Секретной Службой США (USSS) и Университетом Карнеги-Меллона. Были проанализированы 23 киберпреступления, совершенных в период с 1996 по 2002 год сотрудниками банков и финансовых организаций США, причем ряд преступников согласился дать интервью и объяснить мотивы своих действий. В отчете под названием «Угроза изнутри: незаконная компьютерная активность в банковском и финансовом секторах» в качестве главного вывода отмечается, что преступникам, как правило, не потребовались какие-то особые знания и навыки. Для «взлома» систем использовались не столько недостатки оборудования и программного обеспечения, сколько отсутствие должной дисциплины и контроля на рабочих местах. Большинство преступлений было совершено ради наживы, но в четверти случаев основным мотивом была месть — как правило, за увольнение.

- Сотрудники должны знать, что все их действия контролируются. По данным того же исследования, значительная часть преступников не подозревала о существовании в организации системы контроля, и многие из них в своих интервью говорили, что не стали бы нарушать закон, если бы знали, что их могут поймать.
- Кроме кнута должен быть и пряник. Внимательное и человечное отношение руководства к своим сотрудникам — даже такие мелочи, как букет цветов ко дню рождения, — не только снижает вероятность саботажа и диверсий из мести, но и поощряет бдительность лояльных работников.

ПРИМЕР

Из «Стандарта Банка России...»

5.11. Соблюдение политики ИБ в значительной степени является элементом корпоративной этики, поэтому на уровень ИБ в организации серьезное влияние оказывают отношения как в коллективе, так и между коллективом и собственником или менеджментом организации, представляющим интересы собственника. Поэтому этими отношениями необходимо управлять. Понимая, что наиболее критичным элементом безопасности организации является ее персонал, собственник должен всемерно поощрять решение проблемы ИБ [1].

- Необходимо обучение и регулярная переподготовка кадров как по основной деятельности, так и по вопросам информационных технологий, делопроизводства и безопасности.

Опять-таки, угроза криминальных действий со стороны сотрудников —

По данным «Глобального обследования состояния информационной безопасности — 2008», подготовленного компанией PricewaterhouseCoopers, сотрудники и бывшие сотрудники компаний являются виновниками 50% всех инцидентов информационной безопасности. В 2007 г. этот показатель составлял 69%.

не единственная, а часто и не главная из угроз ИБ со стороны персонала. Для организации тяжкие последствия могут повлечь уход (особенно — переход к конкурентам) ключевых сотрудников, или их отсутствие на рабочих местах по болезни или по иным причинам. Для уменьшения уровня этой угрозы необходимо:

1) снижать заинтересованность сотрудников в смене места работы, для чего:

- следить за средними уровнями зарплаты на рынке труда и не допускать заметного отставания уровня зарплаты ключевых сотрудников от средних уровней;
- следить за тем, чтобы у сотрудников всегда была ясная перспектива профессионального роста и/или роста зарплаты;
- не забывать о моральном поощрении сотрудников, о создании хорошего климата в коллективе. Внимательное и человечное отношение к сотрудникам не требует больших издержек, но зачастую дает гораздо больший эффект, чем материальное поощрение;
- развивать корпоративную культуру, включающую лояльность к своей организации,

2) избегать ситуаций, когда сотрудник становится незаменим; своевременно готовить кадровый резерв. Если обстановка в организации благоприятная и сотрудники уверены в своем будущем, в дальнейшем продвижении, — тогда они, как правило, охотно передают свой опыт более молодым коллегам;

3) подробно и тщательно описывать деловые процессы и операции на всех участках, оформляя эти описания в виде внутренних нормативных документов — инструкций по выполнению операций. Цель — обеспечить правильное выполнение действий даже персоналом, незнакомым с данным участком работы. Необходимо также прописать правила передачи полномочий и функций отсутствующих сотрудников.

ПРИМЕР

В декабре 2007 г. все заместители генерального директора и ряд ведущих сотрудников ОАО «Пермэнергосбыт» после проведения аукциона по продаже 49% акций АО блокировали работу компании (ушли на больничный или в отпуска). Им принадлежали ЭЦП, дающие доступ к банкам, к работе на оптовом рынке. Была парализована работа серверной, ключи от которой были «утеряны». После ее вскрытия обнаружилась пропажа 44 дисков, на которых была база данных по всем потребителям города Перми.

Другие уязвимые места в системе информационной безопасности

Если предположить, что службы ИТ, ДОУ, безопасности, кадровая и другие добросовестно выполняют свои служебные обязанности, то уязвимые места в системе ИБ возникают, как правило, или на стыке зон ответственности служб, или там, где необходимо взаимодействие нескольких служб. Чтобы проблемы не возникали или возникали как можно реже, следует руководствоваться некоторыми правилами:

В отношении электронных документов необходимо соблюдать все требования к электронному документообороту.

- в отношении электронных документов необходимо соблюдать все требования к документообороту, включая:

— строгий учет документов, включение электронных документов в номенклатуру дел;

— установление сроков хранения;

— долговременное хранение электронных документов с сохранением их целостности и аутентичности;

— проведение экспертизы ценности и уничтожения электронных документов по истечении сроков хранения в строгом соответствии с законодательством;

- для обеспечения непрерывности деловой деятельности организации и восстановления в случае катастроф необходимо разработать и внедрить планы действий на случай чрезвычайных ситуаций, которые включали бы в себя и планы защиты важнейших

документов организации как электронных, так и бумажных;

- важно обеспечение единой политики управления доступом к документам организации на всех видах носителей;
- необходимо сохранение корпоративной памяти организации в виде документов на всех видах носителей: ее истории, опыта успехов и неудач и т.д. И, наконец,
- обязательна защита конфиденциальной информации и персональных данных.

Распространение на электронные документы правил работы службы ДОУ

Учет документов. Немалую угрозу ИБ создает распространенный, к сожалению, беспорядок в учете электронных документов. Службы ИТ чаще всего отвечают только за регулярное резервирование информации. То, что с информацией и документами нужно работать в строгом соответствии с правилами делопроизводства, они, возможно, слышали, но сами делать этого не умеют и не собираются и, что особенно скверно, не хотят доверить этого тем, кто умеет — специалистам ДОУ (справедливости ради нужно сказать, что и специалисты ДОУ зачастую не хотят брать на себя ответственность за управление электронными документами).

Если в организации имеется маломальски приличная служба ДОУ, то всегда можно получить информацию об объемах бумажных документов, о том, где и какие документы хранятся. Могут ли сотрудники даже очень хорошей службы ИТ столь же подробно рассказать об электронных документах? Как правило, нет, — и это означает, что в системе ИБ есть «дыра»: ведь, для того чтобы обеспечить сохранность информации и документов, необходимо знать, что, в каких объемах, где и сколько времени нужно хранить. Во многих организациях отсутствует даже элементарный учет имеющихся программных средств и баз данных, и в результате электронные документы и информация либо утрачиваются, либо их становится невозможно ни найти, ни использовать. Уничтожение увольняющимися сотрудниками «своих» электронных богатств — тоже распространенное явление, с которым невозможно бороться, если в электронном хозяйстве нет порядка.

Электронная почта. Сегодня электронная почта стала общепринятым средством ведения деловой деятельности и одним из важнейших информационных ресурсов организации. В большинстве стран мира уже решен вопрос о юридическом статусе этих сообщений, да и в России суды уже начали принимать сообщения электронной почты в качестве доказательств.

По американским данным, в настоящее время в среднем 90% интеллектуального капитала компаний хранится в электронном виде, из них 45% постоянно находится на почтовом сервере, часто без всякого контроля и защиты. Если регламенты работы с электронной почтой плохо продуманы с точки зрения обеспечения информационной безопасности и соблюдения законодательно-нормативных требований, организация сильно рискует. Возможны существенные потери как из-за утечки конфиденциальной информации, так и при рассмотрении исков в суде или при проверке ее деятельности контролирующими органами. Не редкость и миллионные штрафы за нарушение правил сохранения электронных сообщений.

ПРИМЕР

16 мая 2005 г. одна из крупнейших инвестиционных компаний мира Morgan Stanley судом США признана виновной в мошенничестве. Штраф, наложенный на компанию, является самым крупным в истории — 1,4 млрд долларов. Главная причина привлечения компании к ответственности — неспособность представить в суд свою электронную переписку.

В настоящее время в среднем 90% интеллектуального капитала компаний хранится в электронном виде, из них 45% постоянно находится на почтовом сервере, часто без всякого контроля и защиты.

***

Всемирный совет автоспорта в сентябре 2007 г. принял решение об исключении команды «Формулы-1» «Макларен» из Кубка конструкторов этого года и оштрафовал на 100 млн долл. за то, что главный конструктор команды был уличен в нелегальном владении секретной технической документацией «Феррари». Компания собиралась подавать апелляцию, однако отказалась от этого, сообщив в официальном пресс-релизе: «К нашему сожалению и удивлению, из содержания электронных писем, о существовании которых ранее не было известно, стало ясно, что доступ к информации не ограничивался одним человеком, хотя это никоим образом не было санкционировано командой» [2].

В большинстве развитых стран сообщения электронной почты признаются деловыми документами и могут быть предъявлены в качестве доказательства в суде.

Аутентичность электронных документов. Еще одна грань информационной безопасности — сохранение аутентичности и целостности электронных документов. Пока что мало кто задумывается о том, смогут ли они использовать свои электронные документы, например, в суде. Но если сегодня не начать архивировать электронные документы в строгом соответствии с известными международными стандартами, то завтра, когда их юридическая значимость станет общепризнанной, организация не сможет доказать подлинность своих документов. Для компаний, ведущих международную деятельность, это уже сейчас «горящая» проблема, поскольку, к примеру, в большинстве развитых стран сообщения электронной почты признаются деловыми документами и могут быть предъявлены в качестве доказательства в суде.

Уничтожение документов с истекшими сроками хранения. Возможность вполне законно уничтожить документы по истечении срока хранения — чрезвычайно важный элемент всей работы по обеспечению информационной безопасности. Это не только возможность уменьшить риск утечки конфиденциальной информации, фактически, — это амнистия старых «грешков» организации, при условии, что у нее хорошо налажены делопроизводство и документооборот.

В бумажном делопроизводстве уничтожение документов и предшествующий этап экспертизы их ценности считаются наиболее сложными видами работ, требующими как высокой профессиональной квалификации, так и умения взаимодействовать практически со всем коллективом организации. С электронными документами нужно решать все те же проблемы, что и с бумажными, плюс еще несколько: порой очень трудно разыскать и уничтожить все имеющиеся копии электронного документа (включая те, что хранятся на резервных лентах), к тому же, как выяснилось на практике, гарантированное уничтожение электронных документов требует физического уничтожения носителей этих документов, для чего требуются специальные технические средства.

Сохранение важнейших документов организации

К важнейшим относят те документы и материалы — на всех видах носителей (необязательно подлинники), которые потребуются немедленно, в первые минуты, часы и дни после чрезвычайного происшествия, а также те, безвозвратная утрата или повреждение которых подрывает (по юридическим, нормативным и эксплуатационным причинам) возможность организации продолжать свою деятельность (п. 7.1. ГОСТ Р ИСО 15489—1-2007) [5]. Важнейшие документы — это необязательно ценные документы постоянного срока хранения. Так, к ним относятся списки телефонов и адресов сотрудников компании, списки поставщиков, способных в случае необходимости предоставить помещения и оборудование, необходимое для восстановления деятельности, и т.п.

[1] «Макларен» решил не опротестовывать решение по скандальному «делу Кофлэна»//Газета.ua. 21.09.2007 http://gazeta.ua

Вопросы защиты важнейших документов выдвинулись на первый план после теракта 11 сентября 2001 г., когда были разрушены башни Всемирного торгового центра (ВТЦ) в Нью-Йорке. Не только американцы, но и представители делового мира из других стран внимательно изучали приобретенный опыт восстановления деловой деятельности. Самыми уязвимыми оказались бумажные документы — практически все они погибли. Большинство располагавшихся в ВТЦ компаний смогли, благодаря хорошо налаженному резервированию в удаленных центрах, практически полностью сохранить электронные документы и информацию. Те из них, кто позаботился о подготовке планов на случай непредвиденных обстоятельств и о тренировках персонала, либо вовсе не прерывали своей деятельности, переключив ее на резервные центры управления, либо смогли быстро вернуться к работе.

В нашей стране защите важнейших документов как составной части плана действий в непредвиденных ситуациях тоже стали уделять внимание как сами организации, так и контролирующие органы. Например, план ликвидации последствий непредвиденных обстоятельств включен ЦБ РФ в перечень обязательных документов кредитной организации как один из документов, регулирующих функции системы внутреннего контроля.

Как и многие другие задачи, проблема защиты важнейших документов решается только в том случае, когда служба ДОУ, отвечающая главным образом за «бумажную» работу, и служба информационных технологий, контролирующая сегодня электронные документы и материалы, действуют согласованно.

Обеспечение единой политики управления доступом к документам

При современном ведении делопроизводства и документооборота с использованием электронных систем есть возможность «прописать» права доступа к каждому конкретному электронному документу. Сплошь и рядом эти права устанавливаются без учета того, как комплектуются в дела соответствующие бумажные документы, — или, напротив, комплектация бумажных документов в дела проходит без учета прав доступа, определенных в системе электронного документооборота. Поскольку в бумажном документообороте пользователь получает доступ сразу ко всем документам, вшитым в дело, то вполне возможна ситуация, когда он может получить доступ к тем документам на бумаге, которые ему не доступны в электронной форме. Бессмысленно защищать электронный документ, если сотрудник имеет возможность без проблем получить его бумажный экземпляр.

Сохранение корпоративной памяти

Когда говорят о сохранении корпоративной памяти, в первую очередь имеют в виду те документы и материалы, сохранение которых не является обязательным по закону. Корпоративная память — важнейший элемент корпоративной культуры, способствующий укреплению лояльности сотрудников, сохранению уникального стиля организации, опыта прошлых успехов и неудач. Корпоративная память, кроме того, представляет собой и важный деловой ресурс, поскольку соответствующие документы и материалы широко используются в целях рекламы и маркетинга. Сохранение корпоративной памяти требует согласованных усилий в первую очередь со стороны служб ДОУ, ИТ и отдела кадров.

Защита конфиденциальной информации и персональных данных

В настоящее время вопросам защиты конфиденциальной информации, и особенно — защите персональных данных, уделяется большое внимание во всем мире. В Европе и в ряде других

Проблема защиты важнейших документов решается только в том случае, когда служба ДОУ, отвечающая главным образом за «бумажную» работу, и служба информационных технологий, контролирующая сегодня электронные документы и материалы, действуют согласованно.

стран уже достаточно давно действуют жесткие законы, регулирующие процессы сбора, доступа и использования подобной информации. Ограничивается объем собираемой информации, возможность передачи или продажи ее третьей стороне и использование ее для маркетинга; от организаций требуется предоставлять клиентам возможность просматривать и корректировать собранную о них информацию; ограничивается срок хранения персональной информации. Требования европейского законодательства об обеспечении безопасности персональных данных настолько жесткие, что это создает трудности при ведении бизнеса. Оно запрещает передавать любые персональные данные в те страны, где отсутствуют такого рода законы и защита — в том числе в США[2]. В Соединенных Штатах основательно защищаются только финансовые и медицинские персональные данные, но наказания за нарушения следуют весьма серьезные.

Нормативный документ о политике безопасности должен быть разработан в организации с учетом ее производственных особенностей и утвержден руководством. Этот документ должны изучить все сотрудники организации, которые имеют доступ к информации.

С 2006 г. подобное законодательство существует и в России. Федеральный закон № 152-ФЗ «О персональных данных» был принят 27 июля 2006 г. Если первое время данный закон практически не работал, то сейчас ситуация изменилась: с одной стороны, граждане и организации начали использовать его для отстаивания своих прав, а с другой — некоторые государственные органы увидели в нем возможность для «закручивания гаек» и навязывания коммерческим организациям разного рода сертификаций, специализированного оборудования и т. д.

ПРИМЕР

В октябре 2008 г. проверкой Управления Россвязькомнадзора по Республике Башкортостан было установлено, что ООО «Мэтр-Вояж», ООО «Алмаз», ООО «Региональный представитель» производили обработку персональных данных своих клиентов (сбор, хранение, использование, передачу и т.д.) без уведомления уполномоченного органа по защите прав субъектов персональных данных (ст. 22 ФЗ «О персональных данных). На руководителей этих организаций составлены три протокола по статье 19.7 Кодекса об административных правонарушениях и направлены в судебные органы.

***

На подъездах домов в селе Амурзете в Октябрьском районе ЕАО появились объявления с предупреждениями о необходимости погашения задолженности за коммунальные услуги. В объявлениях имелся список должников с указанием их фамилий, инициалов, адреса места жительства и суммы задолженности. Граждане обратились в прокуратуру Октябрьского района ЕАО. По результатам проверки прокурором Октябрьского района вынесено постановление о возбуждении дела об административном правонарушении в отношении ООО «Управляющая компания» по ст. 13.11. КоАП РФ — нарушение установленного законом порядка использования или распространения информации о гражданах (персональных данных), по результатам рассмотрения которого постановлением мирового судьи Октябрьского судебного участка ООО «Управляющая компания» признано виновным и ему назначено наказание в виде штрафа в размере 5000 руб [3].

Меры, обеспечивающие информационную безопасность

Главное, что для себя должен решить руководитель, — нужно ли вообще что-то делать для обеспечения информационной безопасности организации, и если да, то нужно ли для этого создавать отдельную службу. Руководитель должен помнить, что если он считает эту работу важной и необходимой, он

[2] Американские компании вынуждены использовать т.н. «зонтичные соглашения», чтобы иметь возможность работать с персональными данными из Европы. В рамках «зонтичного соглашения» американская компания обязуется полностью соблюдать соответствующее европейское законодательство.

[3] Управление Россвязькомнадзора по РБ выявило нарушения в сфере обработки персональных данных/Информационное агентство «Башинформ». — 1 ноября 2008 г. — http:/www.bashinform.ru/

должен обеспечить ей постоянную поддержку и регулярное выделение ресурсов. Без поддержки со стороны высшего руководства организации успеха добиться невозможно.

Стандарты по информационной безопасности рекомендуют создать в организации отдельную службу ИБ. Однако внимательный анализ состояния информационной безопасности в организации обычно показывает, что большинство вопросов успешно решается другими службами организации при исполнении их основных обязанностей. Для закрытия имеющихся «дыр» чаще всего требуется совместные усилия уже существующих служб, а не вмешательство «со стороны». Таким образом, то, в чем реально нуждается организация, — это налаживание совместной согласованной работы имеющихся служб, причем для решения не только проблем ИБ, но многих других задач. Таким координатором может стать сотрудник службы безопасности, или любой энергичный руководитель из других служб организации.

В соответствии со стандартом ISO ГОСТ Р ИСО/МЭК 17799—2005 основные меры, реализация которых позволяет добиться требуемого уровня информационной безопасности организации, включают в себя:

- разработку и проведение в жизнь политики (регламента) информационной безопасности;
- распределение обязанностей по обеспечению информационной безопасности;
- обучение и подготовку персонала по вопросам поддержания режима информационной безопасности;
- внедрение системы уведомлений о случаях нарушения системы безопасности;
- разработку планов на случай чрезвычайных ситуаций и для обеспечения непрерывности деловой деятельности организации;
- защиту документов организации (в том числе важнейших документов);
- защиту персональных данных и информации, являющейся интеллектуальной собственностью.

Руководитель организации должен (рис. 1):

- понимать значимость проблем информационной безопасности, и их взаимосвязь с другими направлениями деятельности, такими как обеспечение соответствия законодательству и нормативным требованиям, управление качеством, обеспечение непрерывности деловой деятельности и т.д.;
- понимать последствия несоблюдения правил информационной безопасности;
- видеть слабые места в информационной безопасности своей организации.

Нормативный документ о политике безопасности должен быть разработан в организации с учетом ее производственных особенностей и утвержден руководством (рис. 2). Этот документ должны изучить все сотрудники организации, которые имеют доступ к информации.

Из исследовательского отчета фирмы «Эрнст и Янг»

Нет более влиятельного фактора, чем высшее руководство, устанавливающее правила игры, которые сводятся к тому, что информационная безопасность имеет большое значение и что конкретные лица, включая руководителей высшего и среднего уровней, должны отвечать за свои действия. Высшее руководство должно осознавать важность информационной безопасности и связанных с нею ограничений. Если же в это не верит высшее руководство, почему это должен делать кто-то другой? [4].

Рис. 1

Из «Стандарта Банка России...»

8.1.2. Политика ИБ должна описывать цели и задачи СМИБ и определять совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется организация в своей деятельности [1].

Рис. 2

Ответственность за обеспечение информационной безопасности несут все руководители организации. Поэтому руководству необходимо регулярно проводить обсуждение проблем защиты информации для выработки четкой единой позиции по этому вопросу, а также для оказания административной поддержки деятельности по обеспечению безопасности. Желательно регулярно рассматривать вопросы обеспечения информационной безопасности на заседаниях коллегиальных органов управления организации.

Литература

1. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. СТО БР ИББС-1.0—2006 (принят и введен в действие распоряжением ЦБ РФ от 26.01.2006 №Р-27)//Вестник Банка России, № 6, 03.02.2006.

2. ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements (Информационные технологии — Методы обеспечения безопасности — Системы менеджмента информационной безопасности — Требования). — ISO. — 2005.

3. ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management (Информационные технологии — Методы обеспечения безопасности — Практика менеджмента информационной безопасности). — ISO. — 2005.

4. Глобальное исследование по информационной безопасности 2004//Исследовательский отчет фирмы «Эрнст и Янг». — 2004. — Сетевая версия http://www. ey. com/global/download. nsf/Russia/CIS_Info_Survey_04R/$file/IntInfoSec2004R. pdf.

5. Глобальное исследование по информационной безопасности 2007//Исследовательский отчет фирмы «Эрнст и Янг». (Global Information Security Survey 2007, Ernst & Young). 2007. — Сетевая версия //www. ey. com/global/assets. nsf/finland/global_information_ Security_Survey_2007/$file/10th%20Annual%20GISS. pdf.

6. Глобальное исследование по информационной безопасности 2008//Исследовательский отчет фирмы «Эрнст и Янг». (Global Information Security Survey 2008, Ernst & Young), 2008. — Сетевая версия http://www. ey. com/global/assets. nsf/international/tsrs_ Global_Information_Security_Suvey_2008/$file/TSRS_Global_Information_Security_Survey_2008.pdf.

Информация для размышления

Охота за персональными данными

Аналитическое исследование «Утечки I полугодия 2008 года», проведенного Infowatch, показало, что самым популярным каналом утечек информации является Интернет, и, по мнению экспертов, доля утечек через глобальную сеть в дальнейшем будет только увеличиваться.

При этом эксперты утверждают, что роль электронной почты в потере информации явно занижена: этот канал должен занимать 2-е место в данном рейтинге.

№ рейтинга	Канал утечки	Доля случаев утечки через данный канал, в % от общего количества случаев
1	Интернет, Интранет	27
2	Ноутбук, КПК	21
3	Неизвестно	14
4	ПК, сервер	13
5	Бумажный носитель	10
6	CD, DVD, флэшка	6
7	Архивный носитель	4
8	Другое	3
9	E-mail	2

Анализируя все упоминавшиеся в СМИ утечки конфиденциальной информации за период с 1 января по 30 июня 2008 г., эксперты пришли к выводу, что наибольший интерес для злоумышленников представляют персональные данные, которые являются в западных странах наиболее востребованной информацией: в 2008 г. было зафиксировано 95% случаев утечки информации, содержащей персональные данные, против 93% в 2007 г. В то же время случаи утечки ноу-хау, коммерческой и государственной тайны, в основном, публично не освещаются в СМИ, поэтому так малы и данные по ним: на утечки коммерческой тайны приходится 2% всех сообщений об утечках, а на государственную тайну — 1%.

Источник: Infowatch