ПРИМЕНЕНИЕ СРЕДСТВ, МЕТОДОВ, ПРИНЦИПОВ ЗАЩИТЫ ИНФОРМАЦИИ при построении информационных систем

Надежда Валерьевна Ручанова, аспирант заочной формы обучения Белорусского государственного университета информатики и радиоэлектроники

При построении информационных систем необходимо не только автоматизировать бизнес-процессы организации, но и обеспечивать бесперебойную работу организации, сведя к минимуму ущерб от событий, несущих риски информационной безопасности путем применения средств защиты информации на всех стадиях создания информационных систем.

При создании информационных систем заказчики обычно руководствуются ГОСТом 34.601-90 «Автоматизированные системы. Стадии создания», предусматривающим следующие стадии: формирования требований к автоматизированной системе: разработка концепции автоматизированной системы, техническое задание, технический проект, эскизный проект, рабочая документация, ввод в действие. В то же время будет ошибочно полагать, что информационная система предприятия или организации создается «с нуля». Как правило, организация уже имеет систему коммуникаций, локальные вычислительные сети, отдельные программные или программно-аппаратные комплексы средств.

Управление информационной безопасностью предприятия предполагает коллективное использование информации, обеспечивая при этом ее защиту (конфиденциальность, целостность, доступность) и защиту вычислительных и сетевых ресурсов на всех уровнях.

Не редкой является ситуация, когда информационная система предприятия создается дискретно: процессом создания руководят разные люди, отсутствует политика информационной безопасности. Чаще всего данный подход приводит к:

- отсутствию системного подхода при проектировании и создании отдельных проектов (систем);
- частичному внедрению разрабатываемых программных средств;
- дублированию элементов проектных решений;
- неспособности реализованных средств и внедренных технологий оптимизировать бизнес-процессы организации.

Рассмотрим следующую ситуацию. В крупной государственной организации, имеющей разветвленную территориальную структуру филиалов в каждом регионе, требуется создать автоматизированную систему мониторинга финансово-хозяйственной деятельности и внедрить систему кадрового учета персонала. В организации в головном офисе есть отдел компьютерного и системного обеспечения, обслуживающий компьютеры и ЛВС. В его состав входят 2 системных администратора и начальник отдела, занимающийся закупками вычислительной техники. Вопросы информационной безопасности ранее не возникали. Руководством организации принимается решение о том, что задачи будут решаться двумя различными внешними исполнителями, при создании информационных систем необходимо соблюсти действующие требования законодательства в области информационной безопасности.

Уровень (аспект) создания системы	Вопросы для обсуждения (решения)
Определение координаторов (ответственных) и исполнителей	Очевидно, что при имеющемся кадровом потенциале организация не в состоянии самостоятельно справиться с поставленной задачей. Таким образом, принимается решение о привлечени к работе сторонних организаций-исполнителей. Для выбора исполнителя необходимо провести конкурсную процедуру из двух ЛОТов. Автоматизация кадрового делопроизводства и учета персонала является типовой для большого количества организаций. Таким образом, для ее решения целесообразно привлечь организацию, имеющую большой опыт в данной области. Как правило, подобные задачи решаются на базе стандартных компонент (например 1С), однако они могут нуждаться в существенной доработке либо настройке в случае, если организация имеет сильно выраженную специфику (государственная служба, военная служба и т. п.). Задача мониторинга финансово-хозяйственной деятельности, несмотря на то, что так или иначе она решается во многих организациях, типовой не является. При выборе исполнителя желательно ориентироваться на организации, имеющие опыт в данной сфере, однако следует понимать, что не всегда опыт может быть применим. В любом случае для написания технического задания опыта ИТ-отдела организации будет недостаточно,, особенно в части описания функциональных требований к системам. Для того, чтобы это стало возможным, необходимо привлекать к участию специалистов кадровой и финансовых служб. Для ускорения процессов согласования решений крайне рекомендуются назначить куратором процесса одного из руководителей предприятия, так как в противном случае трудно ожидать адекватного содействия от специалистов в прикладных областях
Создание транспортного уровня	Создание транспортного уровня предполагает создание локальных вычислительных сетей на центральном и нижестоящих уровнях организации; создание корпоративной сети — объединение локальных сетей, организация соединений с внешними участниками процесса для межведомственного взаимодействия. На этом уровне необходимо определить как риски, которым может подвергаться информация, так и методы, которые будут применяться на данном уровне. На транспортном уровне информационная безопасность может обеспечиваться специальным оборудованием, применением сетевых протоколов. Специалисты должны принять решение, каким образом будет осуществляться связь пользователей системы, учитывая финансовые возможности предприятия. Очевидно, что наиболее качественным и безопасным методом связи являются выделенные каналы доступа, однако их дороговизна делает их широкое применение практически невозможным. Более приемлемым будет аренда каналов, однако следует понимать, что предлагаемые для аренды каналы являются сетями общего пользования и конфиденциальная информация, передаваемая по ним, нуждается в дополнительной защите криптографическими методами
Вычислительные мощности и оборудование, системное программное обеспечение	Часть задач по обеспечению информационной безопасности может быть решена посредством функциональных возможностей оборудования и системного программного обеспечения. Важным при обеспечении непрерывности работы предприятия (доступности информации) является организация серверных групп и систем резервного копирования и восстановления данных. Современное активное сетевое оборудование позволяет обеспечивать функции межсетевого экранирования, шифрования пакетов данных, мониторинга вторжений. СУБД ведущих производителей также позволяют осуществлять широкий круг информационной безопасности
Создание прикладного программного обеспечения	Прикладное программное обеспечение должно интегрироваться со средствами криптографической защиты информации. Так, например, при приеме отчетности в виде электронного документа для обеспечения юридической значимости и целостности необходимо применять электронную цифровую подпись. При сохранности персональных данных необходимо применять шифрование данных и средства защиты от несанкционированного доступа
Кадры	Для эффективного функционирования систем необходимо проводить работу не только с пользователями, эксплуатирующими прикладные модули, но и реформировать существующие кадровые ИТ-структуры предприятия. Так, например, существующие международные правила рекомендуют выделять подразделения, отвечающие за информационную безопасность, из сферы влияния руководителей ИТ-подразделений. Даже в случае выделений функциональных обязанностей для одного сотрудника, например, офицера безопасности, и переподчинения его руководству организации напрямую, может быть существенно снижен риск потери управляемости деятельностью предприятия ввиду того, что критически важная информация сосредоточенна в одних руках

Отдельно отметим, что при построении информационных систем в описанном случае должны использоваться только сертифицированные средства защиты информации, а система должна быть подвергнута аттестации на соответствие требованиям информационной безопасности. ■