Ксения Шудрова, shudrova.blogspot.ru

ЗИ: ИТ или СБ?

На сегодняшний день круг задач специалиста по защите информации достаточно широк: от настройки антивируса до проведения служебных проверок. При этом в каждой организации набор обязанностей такого сотрудника уникальный. Если ранее на предприятии ставки специалиста по ЗИ не было, то при появлении необходимости в собственном защитнике информации, возникает множество споров. Один из главных вопросов – кому должен подчиняться специалист? При этом обычно рассматривают два варианта: отдел информационных технологий (ИТ) и внутреннюю службу безопасности (СБ). Напомним, что понятие «служба безопасности» не применяется к структурным подразделениям в связи с поправками к закону "О частной детективной и охранной деятельности в Российской Федерации". Теперь мы можем встретить только «отделы безопасности» и «службы корпоративной защиты», но для краткости удобнее пользоваться старым определением.

Чтобы поразмышлять о том, какое структурное подразделение должно заниматься защитой информации, необходимо в первую очередь выделить основные особенности работы, как ИТ, так и СБ, а затем проанализировать специфику работы по защите информации.

Для отдела информационных технологий основной задачей является обеспечение бесперебойной работы информационной системы предприятия. Как мы знаем, защиту информации можно условно разделить на обеспечение целостности, конфиденциальности и доступности. Часто к этому списку еще добавляют неотказуемость. Под целостностью понимается отсутствие изменений и искажений в информационных ресурсах. Если для базы данных предприятия обеспечена целостность, количество ячеек и их значения строго определяются действиями, которые производили легальные пользователи. Обеспечение целостности информационных ресурсов является задачей отдела ИТ лишь частично, и включает в себя защиту от непреднамеренных искажений: технических сбоев, чрезвычайных ситуаций. Однако в случае умышленного искажения информации, программисты ничем помочь не смогут.

Что касается конфиденциальности, то здесь все понятно: критичная информация должна оставаться в секрете. Эта задача полностью выпадает из поля деятельности отдела ИТ. Обеспечение доступности информационных ресурсов наоборот является приоритетным направлением работы сотрудников отдела ИТ, а свойство неотказуемости чаще интересует юристов, чем программистов (электронная подпись). В итоге мы имеем

изначальную заинтересованность отдела ИТ лишь в обеспечении доступности ресурсов, а это катастрофически мало для полноценной системы защиты информации.

Рассмотрим, каким образом информационной безопасности может касаться «служба безопасности». Исходя из названия, можно предположить, что задачей структурного подразделения является безопасность во всех ее проявлениях: физическая, экономическая, а информационная?.. Преимуществом решения в пользу выделения ставки специалиста по защите информации в СБ является то, что защищать информацию нужно не только в электронном, но и в бумажном виде, а также те сведения, которые содержат образцы продукции, чертежи, схемы, плакаты, графики. Все это очень трудно увязать с работой отдела информационных технологий. Однако если упустить из виду многообразие форм информации и защищать только электронные сведения, то для нарушителя это будет слишком большим подарком.

Немаловажно помнить широко известный принцип «разделяй и властвуй». Так как работа специалиста по защите информации напрямую связана с проверками, это еще один довод в пользу отнесения его к СБ. В случае подчинения начальнику отдела ИТ, объективность проверок снижается. Ведь мы помним, что самые опасные потенциальные нарушители – системный администратор и программисты. А для того, чтобы контролировать их работу необходимо дистанцироваться, что вряд ли достижимо при работе в одном отделе.

Еще одна особенность работы отдела ИТ заключается в том, что задачи по поддержанию работоспособности локальной сети занимают все рабочее, а иногда и свободное время специалистов и они всегда будут приоритетными для отдела. В то же время процесс защиты информации предполагает установку ограничений в работе. Если у системного администратора приоритетная задача: чтобы все работало быстро, то у безопасника другое правило: система должна быть надежной. Специфика работы программных и аппаратных средств защиты заключается в том, что сочетать эти задачи часто бывает невозможно. Таким образом, мы получаем конфликт интересов внутри одного структурного подразделения, что нежелательно.

«Службы безопасности» предприятий часто обвиняют в консервативном подходе, а также в слепом копировании порядка работы из области защиты государственной тайны. Однако ситуация постепенно меняется в лучшую сторону, все чаще отделом безопасности руководит сотрудник достаточно молодого возраста и прогрессивных взглядов. А на сегодняшний момент прогресс неотделим от информационных технологий, следовательно, защита информации является перспективным направлением работы СБ. Появление ставки специалиста по ЗИ в отеле безопасности смещает ориентиры с

организации пропускного режима в сторону защиты информационных ресурсов. С другой стороны многие «службы безопасности» занимаются экономической безопасностью, в том числе оценкой экономических рисков, применяемые при этом методы оценки во многом подходят для анализа рисков информационных.

Но как и в любой ситуации, кроме явных преимуществ отнесения специалиста по ЗИ к СБ есть и ограничения. Они связаны с тем, что инструменты управления информационной системой находятся полностью в руках отдела ИТ, в частности, системного администратора. Не может специалист по безопасности самостоятельно настроить антивирусную систему, если ему не будут выделены соответствующие права. А значит необходимо организовать эффективное взаимодействие между СБ и ИТ, при этом мостом между этими независимыми подразделениями будет специалист по защите информации. Специалист по ЗИ имеет при этом знания, как в области безопасности, так и информационных технологий и является в этом плане универсалом. Однако самостоятельно решить все возникающие перед ним задачи он не в состоянии, с этой целью и нужно эффективно взаимодействовать с другими подразделениями. О том, как организовать это взаимодействие мы поговорим в следующей статье.