Шудрова К.Е., shudrova.blogspot.ru

Кто поможет специалисту по защите информации?

Часто юный выпускник считает, что справится со всем в одиночку, но это далеко от реальности, хотя бы потому, что у специалиста нет достаточной квалификации в таких предметных областях, как бухгалтерия, экономика, производство. Последнее наиболее важно, изучить специфику производства необходимо обязательно, защита информации сама по себе никому не нужна, как и бухгалтерия – все это лишь инструменты развития бизнеса. В своей работе специалист по защите информации должен использовать сведения обо всех сферах деятельности организации, в первую очередь о характеристиках информационной системы. Специалист по ЗИ не может работать автономно, так как для того, чтобы только создать модель угроз необходимо знать:

- потенциальную стоимость информационных ресурсов;
- топологию сети, характеристики компьютеров и серверов, сетевого оборудования;
- перечень установленного программного обеспечения, сведения об установленной операционной системе, состоянии обновлений;
- должностные инструкции сотрудников (для определения класса возможного внутреннего нарушителя)
- категории информации в системе управления базой данных.

Важно помнить, что если нужна помощь специалистов, то в идеале информация уже должна быть собрана и обработана, а требуется лишь ее экспертная оценка. Утверждение приказов и других локальных документов в области информационной безопасности должно производиться коллегиально. Лист согласования позволяет распределить ответственность и повысить качество разрабатываемого документа (за счет экспертного мнения специалистов в своих областях).

Полезными в этом плане будут производственные совещания по отдельным вопросам. Причем состав специалистов и руководителей, приглашенных для слушания доклада, должен быть тщательно подобран. Важно, чтобы эти люди, действительно могли внести дельные предложения, присутствие сотрудников «для галочки» совершенно ни к чему и только приводит к потере времени при обсуждениях. С другой стороны если забыть одного из экспертов, то, скорее всего, придется собираться повторно. Часто специалист по защите информации входит в состав разнообразных комиссий, как пример – комиссия по классификации информационной системы персональных данных.

Коллектив. Большую роль в работе играет заполнение сотрудниками специальных опросников об особенностях их работы, например для создания режима коммерческой тайны. Составление перечня конфиденциальной информации невозможно без экспертных оценок бухгалтера, экономиста, юриста, кадровика, проектировщика и т.д.

Служба безопасности. Очень важна слаженная работа специалиста по ЗИ и службы безопасности в целом. Физическая безопасность – основа для информационной безопасности. Одно неотделимо от другого. Сигнализация, пропускной режим, видеонаблюдение, внутриобъектовый режим – все это помогает сохранить информацию. В то же время данные, которые хранятся в системах обеспечениях безопасности (записи видео, базы данных пропусков, настройки электронной проходной) должны тщательно оберегаться.

Юристы. По опыту своей работы хочу сказать, что большую часть времени специалист проводит в общении с юристами и специалистами ИТ, чуть меньшую – с бухгалтерией и отделом кадров. С чем могут помочь юристы? К ним стоит обращаться чтения и понимания статей законов, причем, как мы понимаем, юристы на предприятиях имеют довольно широкий профиль и информационное право обычно не является их коньком. А значит, информацию необходимо подавать в удобном виде – сделать выборку нужных статей, благо электронных ресурсов по праву в настоящий момент целое множество. Допустим, необходимо, чтобы юристы помогли разобраться с ответственностью за установку нелицензионных программ. Специалисту по ЗИ следует подготовить выдержки из УК, ГК, КоАП по авторскому праву, изучить и представить судебную практику по данному вопросу. Юристы в этом случае выскажут свое экспертное мнение, поищут решения и постановления, естественно это займет у них меньше времени, чем работа над проблемой без дополнительной информации. Также юридические вопросы возникают при написании официальных писем в контролирующие органы (ФСТЭК, Роскомнадзор, ФСБ и другие).

Руководство. Важно наладить контакт с руководством организации, многие вопросы может разрешить только директор. После того, как документы будут разработаны, а технические средства защиты настроены, необходимо внедрять правила безопасной работы, а здесь никак нельзя обойтись без поддержки руководителей других подразделений и высшего руководства. Защита персональных данных возможно лишь при активном содействии подразделений, контролирующих работу с физическими лицами: отдела кадров и клиентского отдела. Такая простая задача как удаление лишних персональных данных из базы возможна лишь после согласования с руководством, начальником отдела кадров, начальником отдела ИТ.

Интеграторы. Кроме сотрудников помочь в работе могут сторонние организации, например, интеграторы. Если у компании нет соответствующих лицензий, то некоторые виды работы заказываются у фирм, занимающихся защитой информации. Здесь необходимо работать слаженно и участвовать во всех этапах работы. Например, самостоятельно разрабатывать аттестационную документацию, пока производится настройка средств защиты. Это с одной стороны уменьшит стоимость работ, а с другой стороны позволит внутреннему специалисту быть в курсе дела. Часто такие фирмы предлагают в качестве услуги обследование информационной системы – это достаточно дорогая услуга и ее можно сделать самостоятельно, но не всегда для этого есть силы и средства. В некоторых случаях стоит согласиться на такую процедуру, например, если не хватает квалификации (должность новая и образования специализированного нет, опыта работы нет).

Регуляторы. Также как это ни парадоксально звучит – помогут регуляторы, речь идет даже не о проверках, хотя проверки тоже бывают полезны: с их помощью можно понять, что сделано верно, а на что следует обратить внимание. Самое полезное – официальные письма, при четкой формулировке вопроса, мы имеем официальную точку зрения государственного органа, в случае проверок можно опираться на данный документ.

Часто специалисту может быть непонятно, как организовать работу по какому-либо вопросу защиты информации, в этом случае необходимо обращаться за помощью к экспертам в этих областях. Важно отметить, что сотрудничать специалисту по ЗИ предстоит не только с руководителями других подразделений, но и со специалистами в зависимости от того, какие цели преследуются. Если важно дать поручения сотрудникам

другого подразделения или решить организационный вопрос, то стоит обращаться к начальнику отдела, а по чисто техническим вопросам (например, какие персональные данные клиентов собирает организация) лучше консультироваться у специалистов.