Ветер перемен:
и регулятор может ошибаться

Законодательство в области защиты персональных данных не стоит на месте, о чем свидетельствуют последние документы, выпущенные ФСТЭК России. Удивлению специалистов по информационной безопасности не было предела: «ФСТЭК повернулся лицом к операторам!» Такими темпами недолго и до светлого будущего дожить... Но обо всем по порядку.

Евгений Царев |
заместитель директора департамента продуктов и услуг LETA IT-company

Александр Санин |
заместитель руководителя направления ИБ-консалтинга LETA IT-company

В начале года вышли два документа, которые призваны изменить ситуацию в области защиты персональных данных:

- 5 февраля 2010 г. ФСТЭК принял Приказ № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»;
- 5 марта 2010 г. было подписано Решение ФСТЭК, согласно которому упраздняются два руководящих документа: «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных».

Если коротко, то данные документы в значительной степени повлияли на требования к финальным стадиям проектов по защите персональных данных: лицензирование, аттестация и выбор сертифицированных средств защиты информации (СЗИ).

КАК РЫНОК ЭТО ВОСПРИНЯЛ

По большому счету, «четверокнижие» ФСТЭК — это всего лишь рекомендации, т. е. документы необязательные, и разговоры об обязательности выполнения требований «четверокнижия» лишены серьезных юридических оснований. При этом все знают, что с регулирующими органами в России шутить опасно, поскольку большинство необязательных требований могут в один момент превратиться в «обязательные». Поэтому операторы персональных данных последний год готовились к выполнению формальных требований ФСТЭК, а некоторые уже завершили полномасштабные проекты.

Другими словами, рынок воспринял рекомендации регуляторов как обязательные требования. Поэтому факт отмены необязательных документов произвел эффект разорвавшейся бомбы.

В срочном порядке все интеграторы, предоставляющие услуги по защите персональных данных, стали пересматривать свои методологии ведения проектов. А из лагеря операторов доносились облегченные вздохи в стиле: «Ну, наконец-то!».

ПОДРОБНЕЕ О НОВЫХ ДОКУМЕНТАХ

Как обычно бывает, эффект разорвавшейся бомбы недолго длился. После того как рассеялся дым, все заинтересованные лица внимательно взглянули на новые документы.

Если попытаться сделать краткий обзор по Приказу № 58, то можно выделить три принципиальных отличия от «четверокнижия»:

- лицензирование;
- аттестация;
- сертифицированные СЗИ.

Лицензирование

Раньше ходило много споров, нужно ли операторам получать лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации при выполнении проекта по защите персональных данных. Теперь же стало четко понятно, что организации,

проводящие работы по защите персональных данных для собственных нужд и не оказывающие подобные услуги третьим лицам, могут не получать лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации. В случае, если для проведения указанного вида работ организация привлекает стороннюю компанию, привлекаемый исполнитель должен обладать упомянутой лицензией.

Аттестация

Само понятие «аттестация» в Приказе № 58 нигде не фигурирует. Учитывая, что 5 марта было подписано решение ФСТЭК, согласно которому теперь для построения систем защиты персональных данных не нужно применять два методических документа из «четверокнижия», аттестация оказалась изъята из нормативной базы. Другими словами, на сегодняшний день аттестация построенной системы защиты персональных данных не является обязательной (до выхода соответствующего документа).

Сертифицированные СЗИ

Это наиболее сложная и спорная тема. Прямого разрешения на применение несертифицированных СЗИ в приказе ФСТЭК нет. Однако в данном документе четко прописано, что использование СЗИ, прошедших оценку соответствия на отсутствие недекларируемых возможностей (НДВ), является обязательным только для информационных систем персональных данных (ИСПДн) класса К1. Для остальных классов ИСПДн использование СЗИ, прошедших данный вид оценки соответствия, является необязательным и оставляется на усмотрение оператора.

Таким образом, в настоящее время оператор, эксплуатирующий ИСПДн класса ниже К1, для построения системы защиты персональных данных может использовать любые СЗИ, прошедшие сертификацию ФСТЭК по ТУ, что в значительной мере расширяет возможность выбора СЗИ. Тем не менее, при выборе СЗИ необходимо руководствоваться положениями, описанными в «Приложении 1 к положению о методах и способах защиты информации в информационных системах персональных данных».

Все знают, что с регулирующими органами в России шутить опасно, поскольку большинство необязательных требований могут в один момент превратиться в «обязательные»

ВМЕСТО ВЫВОДА

Учитывая, что жестких формулировок в Приказе № 58 нет, стало быть, острота вопроса о технической защите персональных данных в ближайшее время заметно снизится, а проекты в большей степени переместятся в сторону консалтинга, а не внедрения технических средств.

Проекты станут дешевле, однако их количество может увеличиться в разы, и в целом рынок защиты персональных данных должен увеличиться. К тому же «смягчение» требований по использованию сертифицированных СЗИ позволит операторам подойти к их выбору с точки зрения повышения уровня информационной безопасности в целом, а не с позиции наличия/отсутствия сертификата. Теперь стало значительно проще выполнять требования по защите персональных данных в рамках комплексного проекта по повышению уровня информационной безопасности (будь то проекты по СТО БР ИББС, PCI DSS или построение СУИБ). Связано это с исчезновением противоречивых требований и дорогостоящих работ, которые создавали препятствия при выполнении требований других стандартов.