Расширенное заседание комитета по экономической и информационной безопасности НАУФОР

Разработка комплекта типовых документов в области обеспечения информационной безопасности для некредитных финансовых организаций

Управляющая компания и требования Положения № 757-П, ГОСТ Р 57580.1-2018 отраженные в нормативных документах компании по обеспечению информационной безопасности

Андрей Ковешников

Начальник отдела информационных технологий

АО «УК «Регионфинансресурс»

Штат

Где взять столько людей и чем они будут заниматься в обычном режиме?

Ни 250 Указ Президента, ни 235 Приказ ФСТЭК не запрещают нам объединить ИТ и ИБ. Идём в кадры смотреть и редактировать штатное расписание и должностные обязанности сотрудников.

Взаимодействие с внешними сторонами

- С кредитными (банки) и некредитными (спецдепозитарии, брокеры) финансовыми организациями в рамках осуществления компанией операций по управлению активами.
  - Общее нормативное регулирование (применяемы ими уровень защиты информации не ниже чем наш и установлен ЦБ. П. 4.1 Положения 683-П, п. 1.4.1 Положения 757-П);
  - Требование к доведению до своих клиентов рекомендаций по информационной безопасности (п. 7 Положения 683-П, п. 1.13 Положения 757-П) а мы, в свою очередь, должны их выполнять;
  - Использование предоставленного программного обеспечения
- С организациями, неподконтрольными ЦБ РФ:
  - Предоставляющими вычислительные ресурсы от предоставления в аренду виртуальных машин до места для размещения своего оборудования.
  - Предоставляющими различные сервисы.

Соответствие регламентов реальной жизни

- Самыми простыми способами написания регламентов являются прямое цитирование нормативных актов и заимствование готовых. У них есть как плюсы, так и минусы.
- К плюсам следует отнести:
  - Документы вычитаны, опробованы на практике и, даже, возможно, прошли проверку регулятором.
  - Если вы будете отслеживать источник публикации, то как-минимум вы уже как-то выполните требование по постоянному повышению уровня информационной безопасности.
  - Сотрудники случае расхождений документов с жизнью просигнализируют об этом.
- Минусы, которые могут всё испортить:
  - Невозможность исполнить заявленные требования.
  - Ошибка, выявленная у кого-то, позволяет целенаправленно искать её у вас.
  - Ляпы.
- Собственная разработка внутренних нормативных актов с нуля сопряжена с:
  - Значительными временными затратами с отвлечением сотрудников от выполнения непосредственных обязанностей;
  - Соответствующей квалификацией персонала;
  - Необходимостью постоянно отслеживать изменения в законодательстве и актуализировать внутренние документы;
  - Отсутствие уверенности, что всё сделано «Правильно». Как минимум это определение предъявляемых требований, как максимум все действия регламентированы и любое отклонение стопорит процесс.

Оценка программного обеспечения

Пунктом 1.8 Положения 757-П для организаций обеспечивающих минимальный уровень защиты информации предусмотрен выбор между сертификацией и оценкой соответствия используемого прикладного программного обеспечения.

Целесообразно разделить подходы к оценке в зависимости от источника происхождения ПО:

- Получено от контрагента в рамках обеспечения бизнес-процессов компании (банк-клиент, торговый терминал). Здесь надо просить документы у контрагента.
- Приобретённое решение. Тут бал правят поставщики и нам приходится довольствоваться тем, что есть.
- Заказная разработка или собственное ПО. Характеризуется различными взглядами на процесс со стороны заказчика, который уверен, что полностью контролирует процесс и результат, и исполнителя, чья позиция характеризуется не столько крылатой фразой «быстро, дёшево, качественно – выберете любые два», сколько ограничениями накладываемыми непосредственно согласованной процедурой реализации проекта. Требования к информационной безопасности должны закладываться на этапе формирования требований и проверяться на уязвимости на этапе проектирования решения.

На текущий момент остаются открытыми следующие вопросы:

1) Реализация импортозамещения и компенсационных мер;

2) Что делать с явно не попавшими под нормативное регулирование сегментами.

Ожидаем скорейшего утверждения Комитетом по экономической и информационной безопасности НАУФОР Комплекта типовых документов в области обеспечения информационной безопасности для некредитных финансовых организаций.