Алгоритм действий
при формировании требований согласно 31-му приказу ФСТЭК

Руслан СТЕФАНОВ,
руководитель направления защиты АСУ ТП, ОАО «ЭЛВИС-ПЛЮС»

18 августа 2014 г. вступил в силу 31-й приказ ФСТЭК «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». Благодаря активной и открытой позиции ФСТЭК работа над этим документом, в которой принимали участие эксперты по информационной безопасности, получила широкую известность и привела к положительному результату.

Теперь настало время опробовать положения данного приказа на практике. Цель данной статьи – предоставить читателю пошаговую карту действий на первом этапе защиты информации в АСУ ТП в соответствии с 31-м приказом.

Итак, первый шаг – формирование требований к защите информации в АСУ ТП. На рисунке представлена схема, визуализирующая и детализирующая этот процесс.

Прежде всего, заказчик или оператор КВО должен принять решение о создании системы обеспечения безопасности информации (СОБИ). Честно говоря, не знаю, каким образом подобные решения принимаются, единолично руководством или коллегиально на собрании, но наша работа как системного интегратора в области ИБ начинается там, где это решение уже принято.

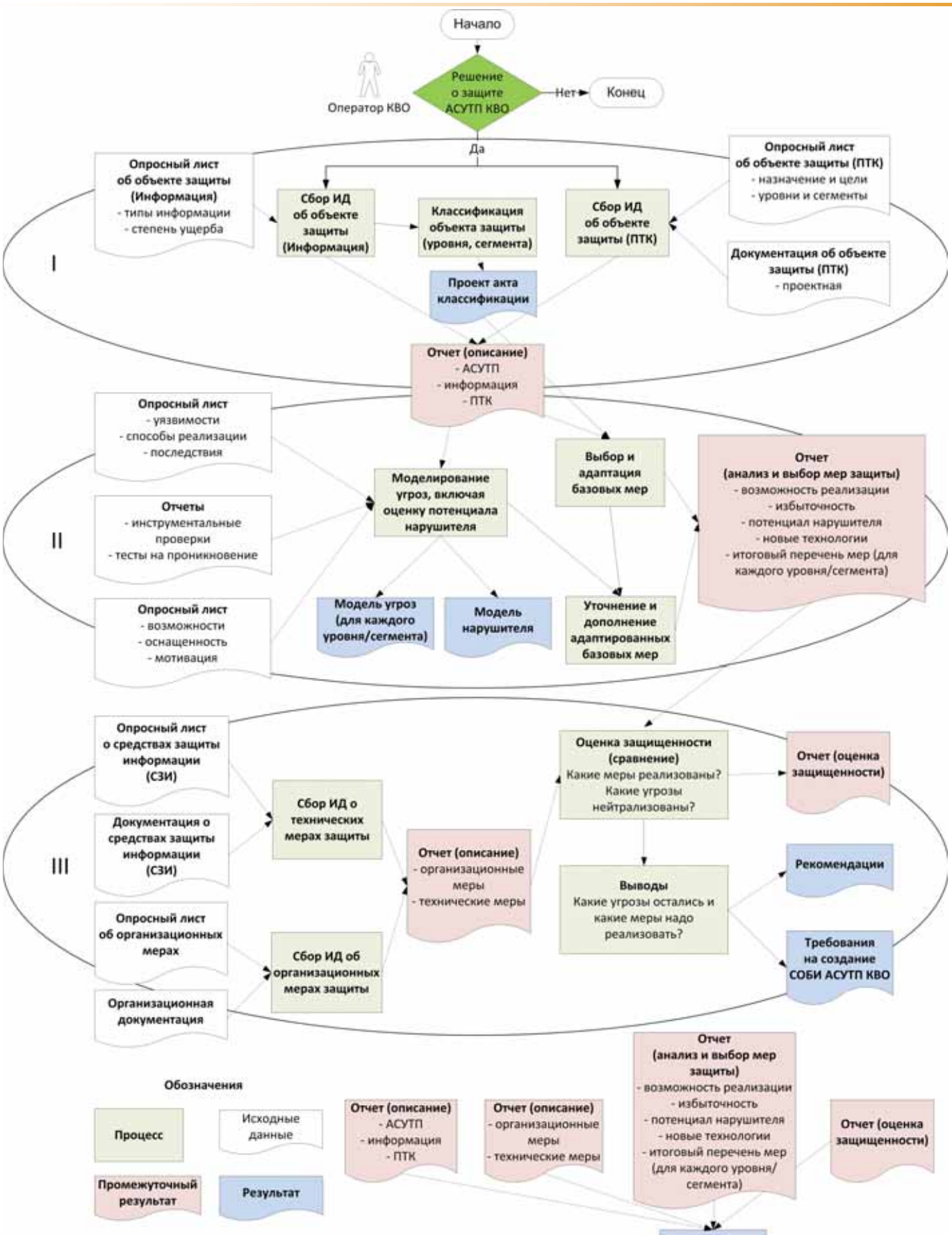
Первая группа работ связана с первоначальным сбором из опросных листов и имеющейся документации исходных данных об объекте защиты (информации и программно-техническом комплексе) – определяются уровни, при необходимости выделяются отдельные сегменты АСУ ТП. В результате заказчик или оператор КВО получает проекты актов классификации уровней и сегментов своей АСУ ТП, которые в дальнейшем нужно утвердить специальной комиссией и использовать для построения системы защиты КВО на базе соответствующего классу набора мер защиты информации. Другой важный результат этих работ – первая описательная часть отчета об аудите АСУ ТП, которая необходима как для построения модели угроз, так и для обоснованного выбора базового комплекса мер защиты информации.

Вторая группа основана на результатах предыдущих работ, отчетах о проведенных тестах на проникновение, а также на инструментальных проверках. При помощи опросных листов на этом этапе собираются данные для формирования карты угроз безопасности информации и потенциала нарушителя. Полученные модели угроз и нарушителя позволяют уточнить и дополнить полученный ранее по акту классификации адаптированный базовый набор мер защиты. Кроме того, отчет об аудите дополняется анализом и выбором мер защиты для каждого уровня и сегмента АСУ ТП КВО.

Третья группа работ является самой важной с точки зрения процесса защиты, так как позволяет оценить защищенность объекта и сделать выбор последующих мероприятий для защиты АСУ ТП КВО. Здесь происходит сравнение существующих организационных и технических мер защиты с выбранными на предыдущем этапе необходимыми для определенного класса защищенности мерами. Для этого собирается информация и даются ответы на вопросы:

- какие меры уже реализованы;
- какие угрозы нейтрализованы данными мерами;
- какие угрозы остались актуальными;
- какие меры необходимы для их нейтрализации.

В результате формируются рекомендации и требования на создание СОБИ АСУ ТП КВО. Еще один значимый результат этого этапа работ – итоговый отчет об аудите, содержащий кроме перечисленного выше описание существующих на момент аудита организационных и технических мер, а также оценку защищенности. Данный отчет пригодится при выполнении следующего аудита для повышения его эффективности и снижения затрат на его проведение.



Надеюсь, представленный на схеме алгоритм действий будет полезным приложением к тексту 31-го приказа ФСТЭК для всех заинтересованных в области защиты АСУ ТП читателей. ■