



Реализация процесса №3 ГОСТ 57580. Управление уязвимостями на аутсорсинге

Введение в проблематику

Требования регуляторов и контроль исполнения

Как осуществляют контроль по 382-П:

▲ 7 точек контроля касаются поиска и устранения уязвимостей



И вот сейчас с введением ГОСТ 57580:

▲ Отдельный процесс из 8ми посвящен контролю целостности и защищенности информационной инфраструктуры

Требования должны быть выполнены к 01.01.2021



Управление уязвимостями

Как делают



Сканирование

Объекты защиты внутреннего периметра сканируются эпизодически

Сканирование



Устранение



Устранение

Обнаруженные уязвимости устраняются, но процесс не систематизирован и не контролируется

+1%

К итоговой оценке по ГОСТ 57580

Управление уязвимостями

Как надо делать

Инвентаризация

Организуется сбор максимально подробных данных об инфраструктуре, чтобы минимизировать ложные срабатывания и лучше понимать «своего клиента»



Контроль

Качество устранения уязвимостей контролируется повторной проверкой до тех пор, пока уязвимости не будут закрыты



Устранение

Исполнитель, назначенный ответственным проводит работы по устранению уязвимости и оповещает о завершении



Сканирование

Объекты защиты внутреннего периметра сканируются в соответствии с расписанием (от ежедневно до ежегодно). Внешние адреса и веб-ресурсы сканируются ежедневно



Анализ

Результаты ранжируются и превращаются в список конкретных задач по устранению уязвимостей для выполнения ИТ-специалистами



Планирование

Для каждой задачи назначается исполнитель и задается срок выполнения



Управление уязвимостями

С использованием аутсорсинга

Инвентаризация

Подрядчик организует сбор максимально подробных данных об инфраструктуре, чтобы минимизировать ложные срабатывания и лучше понимать «своего клиента»

Контроль

Качество устранения уязвимостей контролируется **Подрядчиком** до тех пор, пока уязвимости не будут закрыты

Устранение

Исполнитель, назначенный ответственным проводит работы по устранению уязвимости и оповещает **Подрядчика** о завершении



Сканирование

Объекты защиты внутреннего периметра сканируются **Подрядчиком** в соответствии с расписанием (от ежедневно до ежегодно). Внешние адреса и веб-ресурсы сканируются ежедневно

Анализ

Результаты ранжируются и превращаются **Подрядчиком** в список конкретных задач по устранению уязвимостей для выполнения ИТ-специалистами **Заказчика**

Планирование

Для каждой задачи назначается исполнитель и задается срок выполнения

Управление уязвимостями

Вместо выводов

УПРАВЛЯТЬ УЯЗВИМОСТЯМИ НАДО!



**Сделать все
самостоятельно**



**Выбрать
аутсорсинг**

Благодарю за внимание!

Контактная информация

sales@acribia.ru

*БЦ «Central Yard», офис 43
105005, Бауманская ул., д. 9,
Москва
+7 (495) 640-47-10*

*БЦ «Петровский Форт», офис 641
194044, Финляндский пр-т, 4А,
Санкт-Петербург
+7 (812) 612-00-12*