Как правильно ответить на вопросы аудитора

Содержание

- Головные боли аудитора
- Откуда аудитор берёт вопросы
- Трудности интерпретации нормативной базы
- Оптимизация взаимодействия с аудитором
- Составление корректных ответов
- Выводы

Ситуация

- Вы – специалист по информационной безопасности в банке
- Вас ~~заставили~~ попросили взаимодействовать с аудитором

Головные боли аудитора

- Сроки проекта
- Отсутствие знаний об инфраструктуре
- Разрешение недопониманий

Откуда аудитор берёт вопросы

- Стандарты
- Федеральные законы
- Внутренняя документация Организации
- Опыт проведения аудитов

Интерпретация положений стандартов

Положение ГОСТ 57580.1-2017

Мера РИ.9

- Выделение в составе ГРИЗИ следующих основных ролей:

  - руководитель ГРИЗИ, в основные функциональные обязанности которого входит обеспечение оперативного руководства реагированием на инциденты защиты информации;

  - оператор-диспетчер ГРИЗИ, в основные функциональные обязанности которого входит обеспечение сбора и регистрации информации об инцидентах защиты информации;

  - аналитик ГРИЗИ, в основные функциональные обязанности которого входит выполнение непосредственных действий по реагированию на инцидент защиты информации;

  - секретарь ГРИЗИ, в основные функциональные обязанности которого входит документирование результатов реагирования на инциденты защиты информации, формирование аналитических отчетов материалов

Запрос аудитора

- Формируется ли в Банке группа реагирования на инциденты ИБ?
- Если да, то в каких документах отражены правила её создания и роли в ней?
- Можете прислать этот документ?

Интерпретация положений ЦБ и федеральных законов

Положение ЦБ РФ 382-П

- При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают контроль (мониторинг) соблюдения установленной технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры

Запрос аудитора

- В каких внутренних документах определен порядок работы с электронными сообщениями?
- Можете прислать эти документы?
- Контролируется ли процесс работы с электронными сообщениями?
- Можете прислать акты контроля?

Оптимизация взаимодействия с аудитором

- Если какая-то форма взаимодействия удобнее для Вас, предложите использовать её
- Если вопросы непонятны, уточняйте
- Игнорирование либо перенос сроков не работают (аудит всё равно придётся проводить)

Отвечаем на запрос документации

- Предоставить документ, в котором отражен порядок настройки учетных записей пользователей и администраторов
- Что делать, если нужного документа нет?

Отвечаем на запрос технических свидетельств

- Предоставить конфигурационные файлы сетевых устройств (межсетевые экраны, маршрутизаторы, прокси-серверы), расположенных в исследуемом сегменте
- Если у Вас нет доступа к необходимой инфраструктуре, решайте вопрос с руководством
- Если запрашивают логи, решает не объём, а репрезентативность

Отвечаем на запрос с устными ответами

Вопросы, подразумевающие ответ «Да»/«Нет»

- Применяются ли в Банке съемные носители информации?

Вопросы, подразумевающие развернутый ответ

- Каким образом организован процесс выявления и устранения уязвимостей?

Согласовываем результаты аудита

- Посмотрите, верно ли интерпретировали Ваши интервью
- Узнайте, какая оценка нужна и каким образом её улучшить

Выводы

- Аудитор всегда доступен для взаимодействия
- Если что-то неясно, лучше уточнить
- Предпочтительнее отвечать развёрнуто

Спасибо за внимание!

Автор: Валерий Кунавин

Консультант по информационной безопасности RTM GROUP

RTM GROUP

Объединяем IT, право и безопасность

- Информационная безопасность
- Компьютерно-технические экспертизы
- Юридические услуги в области ИТ и ИБ

info@rtmtech.ru