На основании описанных ситуаций сформулируйте перечень устройств, которые требуется проанализировать для расследования указанных компьютерных инцидентов, а также список вопросов, на которые требуется получить ответы в ходе экспертизы для того, чтобы сделать обоснованные выводы об обстоятельствах случившегося.

Вариант 1.

Конфиденциальная переписка руководителя компании N, связанная с заключением новых контрактов с поставщиками и их обсуждением с рядом сотрудников оказалась размещенной в открытых источниках в сети Интернет. Исходя из состава и текстов опубликованной переписки, можно заключить, что скомпрометирована именно учетная запись электронной почты руководителя. В качестве основного подозреваемого рассматривается системный администратор организации, ранее привлекавшийся для установки корпоративных программ на личный ноутбук руководителя. Помимо ноутбука руководить пользуется смартфоном, планшетом и домашним настольным компьютером. Для подключения к сети Интернет этих устройств – за исключением домашнего компьютера – он использует подключение через свой смартфон. У системного администратора имеются ноутбук и смартфон, для подключения к сети Интернет он использует мобильный интернет или общедоступные Wi-Fi-сети, включая сеть компании N.

Требуется подтвердить или опровергнуть факт компрометации ноутбука руководителя и его почтового ящика, подтвердить или опровергнуть причастность системного администратора, выявить иные возможные каналы утечки электронных писем руководителя.

Вариант 2.

Офис компании N оборудован по принципу «умного дома» рядом устройств интернета вещей. В один из рабочих дней была зафиксирована попытка DDoS-атаки на веб-сервер компании. При первичном анализе журнала регистрации межсетевого экрана были обнаружены IP-адреса некоторых из таких устройств, а именно датчика движения, отвечающего за включение и выключение освещения, а также датчика температуры воздуха, контролирующего систему

кондиционирования. Установку и настройку данных устройств осуществляли специалисты компании-поставщика, а также системный администратор компании N. В процессе работы все участники использовали ноутбуки, а также личные смартфоны.

Требуется определить, была ли атака организована поставщиками устройств или их сотрудниками, сотрудниками компании N или посторонними лицами, а также установить, каким образом контролировались участвовавшие в атаке устройства.