ЧЕК-ЛИСТ «КАК ПРАВИЛЬНО РЕАГИРОВАТЬ НА ИНЦИДЕНТЫ ИБ»

УЦСБ SOC

1. Локализовать и отключить **зараженный сегмент, хосты, АРМы, серверы** от инфраструктуры

2. Провести аудит **запланированных задач** и удалить те, которые были созданы неправомерно

3. Принудительно выполнить смену **аутентификационных данных** всех учетных записей организации

4. Сохранить **журналы событий** со скомпрометированных ИС, контроллеров домена, МЭ, сетевого оборудования, средств защиты информации для обеспечения полноты доказательной базы

5. Снять **дампы памяти** и реестра со скомпрометированных хостов перед восстановлением ИС из бэкапов и проведением антивирусной проверки

6. Провести **аудит** на наличие установленных нелегальных **утилит** или **ПО удаленного доступа**

   Выполнить удаление утилит или ПО удаленного доступа со всех АРМ и серверов организации

7. Обновить базы **антивирусного ПО** и выполнить антивирусную проверку всех АРМ и серверов

   Проверку можно проводить как штатным установленным антивирусным ПО, так и с применением утилит антивирусного ПО

8. Выполнить **поиск характерных файлов и артефактов** на хостах инфраструктуры

   Если есть информация об APT, эксплуатируемых уязвимостях или применяемых злоумышленниками инструментов

9. Запретить на МСЭ **доступ** к relay-серверам ПО удаленного доступа

   Организовать запрет с применением правил фильтрации на локальных межсетевых экранах по включенному в домен имени ПО, либо блокируя адреса на периметровых межсетевых экранах. Перечень адресов требует актуализации на постоянной основе.

   На сетевом оборудовании настроить мониторинг обращений с хостов организации к запрещенным адресам. Запретить использование программ удаленного доступа доменными политиками

10 При компрометации хостов администраторов заблокировать **привилегированные учетные записи**, выполнить настройку отдельных «чистых» АРМ для ограничения доступа к критическим инфраструктурам

«Чистый АРМ» — АРМ, настроенный с минимальным набором необходимого ПО, с установленным обновленным антивирусным ПО. Под критическими инфраструктурами подразумевается виртуализация, системы резервного копирования и т.д.
Запретить удаленный доступ к данным АРМ

11 Ввести **политику** по расширенному аудиту работы ОС

Настроить расширенное логирование на серверах контроллера домена. Выполнить расширенную настройку аудита для серверов Linux, сетевого оборудования и сервисов, используемых в организации (confluence и другие)

12 Выполнить **обновление безопасности** используемых ОС на всех серверах и организовать автоматическое обновление с внутренних серверов WSUS

13 Провести аудит и отключение **сервисов**, не являющихся необходимыми

Это уменьшает поверхность потенциальной атаки и сокращает логируемую и анализируемую информацию

14 Провести аудит и отключить **неиспользуемые порты** на хостах с удаленным доступом

15 **Обратиться в организацию, специализирующуюся на проведении расследований инцидентов информационной безопасности. Например, в УЦСБ.**
