

???? ????????????? ?
????????????????

ИАФ.0 Разработка политики идентификации и аутентификации

Мера ИАФ.0 закрывается разработкой внутренних нормативных документов (это могут быть правила, процедуры и политики), в которых описывается процесс идентификации и аутентификации субъектов доступа и объектов доступа.

ИАФ.1 Идентификация и аутентификация пользователей и иницилируемых ими процессов

Для закрытия данной меры используются механизмы аутентификации ОС и приложений, а также СЗИ от НСД на АРМ операторов и инженерных станциях, в случае организации удаленного доступа нужно использовать VPN/шлюз доступа + MFA, при необходимости РАР.

Платформа KICS не является универсальным механизмом проверки личности пользователя и аутентификации запускаемых им процессов. Частично мера покрывается платформой KICS в части:

KICS for Nodes и KICS for Linux Nodes

Мера ИАФ.1 реализуется в задаче «Контроль запуска программ» в части идентификации пользователей при запуске программ. В параметрах задачи можно указать пользователей или группу пользователей, которым разрешается или запрещается запуск программ.

KICS for Networks

Мера реализуется в части идентификации устройств по MAC- и IP-адресам в обрабатываемой копии сетевого трафика и данных телеметрии от KEA. При этом ведется составление и обновление таблицы устройств с информацией о них.

???2 ????????????? ? ????????????? ?????????

Для реализации меры ИАФ.2 в АСУ ТП должна быть обеспечена возможность идентифицировать подключаемое к информационной системе устройство и подтвердить подлинность его идентификатора. Например, нужно использовать МСЭ для ограничения взаимодействий по портам, адресам, VLAN и другим поддерживаемым атрибутам, а также использовать NAC совместно с коммутаторами, поддерживающими 802.1X и криптографическая аутентификацию, где возможно.

Частично мера закрывается платформой KICS в части:

KICS for Nodes и KICS for Linux Nodes

Мера реализуется в части идентификации устройств по IP-адресам путем выполнения задачи «Защита от сетевых угроз» и «Управление сетевым экраном».

KICS for Networks

Мера реализуется в части идентификации устройств по MAC- и IP-адресам в обрабатываемой копии сетевого трафика и данных телеметрии от KEA. При этом ведется составление и обновление таблицы устройств с информацией о них.

Для усиления требований Приказа №239 нужно использовать встроенные механизмы защиты информации в части идентификации и аутентификации пользователей, которые являются сотрудниками субъектов КИИ, чтобы обеспечить безопасность следующих систем: операционных систем, прикладного программного обеспечения, программируемых логических контроллеров, активного сетевого оборудования и т.п. Данные требования позволяет реализовать операционная система Astra Linux Special Edition, которая также совместима с решениями платформы KICS.

???3 ?????????? ????????????????

Для реализации данной меры используются встроенные механизмы защиты информации, системы защиты информации от несанкционированного доступа (далее – СЗИ от НСД), межсетевые экраны (МЭ, FW), системы управления учётными данными и доступом (далее – IAM-системы).

Частично для контроля и обнаружения изменений в версии KICS for Networks 4.5 появилась функция «[Контроль пользователей на устройствах](#)». Она собирает сведения об учётных записях устройств, отображает идентификаторы безопасности (SID), состояние и блокировку учётных записей, а также регистрирует события добавления, изменения и удаления пользователей. Эта функция лишь дополняет процесс управления идентификаторами, но не реализует покрытие данной меры.

???4 ?????????? ?????????? ????????????????

Для реализации данной меры используются встроенные механизмы защиты информации, а также службы каталогов, СЗИ от НСД, системы управления жизненным циклом сертификатов открытого ключа. Нужно организовать полный жизненный цикл средств аутентификации: выдачу, привязку к учётной записи, замену, блокирование при компрометации и отзыв или уничтожение при прекращении использования.

???5 ?????????????? ? ?????????????? ??????? ????????????????

Для реализации данной меры используются механизмы аутентификации внешних пользователей на шлюзе и целевых системах, а также регламентом предоставления и отзыва доступа. Например, VPN-шлюз с индивидуальными учётными записями, а также использование РАМ систем / шлюзов привилегированного доступа.

???6 ?????????????? ????????????????

Для реализации меры нужно обеспечить взаимное подтверждение подлинности взаимодействующих сторон до предоставления доступа или установления защищённого соединения. Можно использовать PKI и сертификаты, IPsec с взаимной аутентификацией, VPN с сертификатами

???.7 ?????? ?????????????????????? ??????????? ??? ??????????

Для реализации данной меры нужно использовать VPN или другой защищённый канал с корректной аутентификацией. Для поддерживаемых протоколов включить TLS/mTLS или другой предусмотренный механизм защиты. Для сертификатов организовать контроль срока действия, замену и отзыв при компрометации.

Revision #3

Created 21 September 2025 19:24:38 by Olga Sinotova

Updated 21 October 2026 15:27:15 by Olga Sinotova