

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

???0 ?????????? ?????????? ??????????

Мера УПД.0 закрывается разработкой внутренних нормативных документов (это могут быть правила, процедуры и политики), в которых описывается процесс управления доступа.

???1 ?????????? ?????????? ??????????

Мера УПД.1 реализуется комплексно: для её выполнения необходимы как организационные, так и технические меры. В частности, в Политике информационной безопасности следует закрепить общие требования к управлению доступом, а в инструкции для администратора — определить порядок управления учётными записями.

Для технической реализации меры применяются встроенные механизмы защиты информации. Например, Microsoft Active Directory позволяет централизованно управлять учётными записями и группами. Дополнительно могут использоваться системы управления привилегированным доступом (PAM) и средства защиты информации от несанкционированного доступа (СЗИ от НСД).

Kaspersky Security Center (KSC) позволяет централизованно управлять настройками и политиками безопасности продуктов «Лаборатории Касперского».

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

Для полного выполнения этой меры необходим комплексный подход, включающий разработку организационно-распорядительной документации и внедрение технических средств защиты информации.

Важным элементом является матрица доступа, в которой сопоставляются роли и должности с информационными ресурсами и функциями. Для каждой пары следует указать требуемый уровень доступа: чтение, запись, выполнение или отсутствие доступа.

Для технической реализации меры используются встроенные механизмы защиты информации. Например, в Microsoft Active Directory управление доступом на основе ролей (RBAC) можно реализовать с помощью групп безопасности. Также применяются средства защиты информации от несанкционированного доступа (СЗИ от НСД), поддерживающие дискреционную и мандатную модели управления доступом (MAC), маркировку файлов, а также контроль запуска программ и доступа к съёмным носителям.

На сетевом уровне на межсетевых экранах настраиваются списки контроля доступа (ACL), ограничивающие обмен трафиком между сегментами и ролями в соответствии с установленными правилами.

KICS for Nodes

Мера реализуется в части:

- отслеживания и ограничения доступа пользователей и групп пользователей к заданным файлам и папкам с помощью задачи «Мониторинг файловых операций»;
- отслеживания и ограничения доступа пользователей и групп пользователей к запуску программ с помощью задачи «Контроль запуска программ»;
- отслеживания и блокирования действий пользователей и групп пользователей к указанным ветвям и разделам реестра с помощью задачи «Мониторинг доступа к реестру»;
- отслеживает и блокирование попыток подключения внешних устройств к защищаемому устройству с помощью задачи «Контроль устройств».

KICS for Linux Nodes

Мера реализуется в части:

- отслеживания и ограничения доступа пользователей к заданным файлам и папкам с помощью задачи «Контроль целостности системы»;
- Технологические ограничения операционной системы Linux не позволяют приложению определять, какой пользователь или процесс внес изменение в файл;
- отслеживания и ограничения доступа пользователей к запуску программ с помощью задачи «Контроль приложений»;
- отслеживает и блокирование попыток подключения внешних устройств к защищаемому устройству с помощью задачи «Контроль устройств».

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

Для реализации данной меры используются средства доверенной загрузки (далее - СДЗ), предназначенные для автоматизированных рабочих мест/серверов сотрудников субъектов КИИ и специализированным средствами для доверенной загрузки компонентов среды виртуализации. Также используются СЗИ НСД, имеющие действующий сертификат ФСТЭК. Они внедряются в процесс загрузки и проверяют контрольные суммы (хэши) всех его этапов.

???4 ?????????? ?????????? (?????) ??????????????

Для реализации данной меры используются встроенные механизмы защиты информации, а также системы контроля действий привилегированных пользователей и СЗИ от НСД.

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

Пользователям, процессам и устройствам следует предоставлять только те права доступа, которые необходимы для выполнения их функций, не допуская предоставления избыточных привилегий. Для реализации этого требования необходимо разработать матрицу доступа, по возможности включив её в проектную документацию на АСУ ТП. Также следует установить порядок предоставления прав: доступ предоставляется на основании служебной записки, содержащей обоснование необходимости, и после согласования с руководителем.

Техническая реализация меры предусматривает применение средств защиты информации от несанкционированного доступа (СЗИ от НСД) и настройку встроенных механизмов разграничения доступа используемых систем.

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

Основная ответственность за реализацию УПД.6 возлагается на операционные системы, Active Directory и организационно-распорядительную документацию.

KICS for Nodes

Для рабочих мест под управлением Windows мера реализуется с помощью KICS for Nodes. Попытки подбора пароля выявляются путём анализа журналов событий Windows с использованием задачи «Анализ журналов».

???7 ?????????????? ?????????????? ??? ??? ??????? ? ????????????????? ?????????

Для реализации данной меры используются встроенные механизмы защиты информации.

???8 ?????????? ?????????????? ??? ??????? ?????? ? ?????????? ??????? ? ????????????????????? ???????

Для реализации данной меры используются встроенные механизмы защиты информации, а также СЗИ от НСД, где включена функция «Информирование о предыдущем входе».

Kaspersky KUMA

Мера реализуется в части:

- Настройки аудита с помощью групповой политики на устройстве Windows путем отслеживания «Аудита входа в систему» и «Аудита событий входа в систему».
- Настройка политики аудита на устройстве Windows путем отслеживания «Аудита входа в систему» и «Аудита событий входа в систему».

???9 ?????????????? ?????? ?????????????? ??????? ???????

Мера предусматривает техническое ограничение одновременного входа одного пользователя с нескольких рабочих мест или в несколько окон либо сеансов. Для её реализации могут применяться встроенные механизмы защиты информации, средства защиты от несанкционированного доступа, а также службы каталогов LDAP или Microsoft Active Directory.

При работе с привилегированными учётными записями рекомендуется использовать РАМ-систему в качестве единой точки доступа. Она позволяет контролировать и записывать привилегированные сеансы, а также настраивать запрет на одновременное использование одной учётной записи несколькими администраторами.

???10 ?????????????? ?????? ??????? ?????????????? ??? ??????????????

Система должна автоматически блокировать экран или завершать пользовательский сеанс по истечении установленного периода бездействия, например 5–10 минут. Для

возобновления работы пользователь должен пройти повторную аутентификацию, например ввести пароль.

Для реализации этой меры могут применяться встроенные механизмы защиты информации, средства защиты от несанкционированного доступа (СЗИ от НСД), а также системы контроля действий привилегированных пользователей.

???11 ?????????? ?????????? ?????????????? ?? ?????????????? ? ???????????????

Неаутентифицированному пользователю должны быть недоступны любые действия в системе, за исключением инициирования процедуры входа — ввода учётных данных.

Для реализации этой меры применяются встроенные механизмы защиты информации и средства защиты от несанкционированного доступа (СЗИ от НСД).

???12 ?????????? ?????????? ?????????????

Атрибуты безопасности — это метки и параметры, назначаемые субъектам (например, пользователям и процессам) и объектам (например, файлам, устройствам и сетевым ресурсам). На основании этих атрибутов система принимает решения о предоставлении доступа. К таким атрибутам относятся, например, роль пользователя, уровень конфиденциальности файла или статус устройства в сети. Система должна обеспечивать защиту атрибутов при их создании, изменении и удалении.

Для реализации этой меры применяются встроенные механизмы защиты информации и средства защиты от несанкционированного доступа (СЗИ от НСД). Такие средства позволяют назначать метки конфиденциальности файлам и процессам, а также предотвращать изменение атрибутов защищаемых объектов пользователями, не обладающими соответствующими правами. Кроме того, меру можно реализовать с помощью служб каталогов LDAP или Microsoft Active Directory.

???13 ?????????? ?????????? ?????????? ???????

Любой удалённый доступ к значимому объекту критической информационной инфраструктуры (КИИ) — как из-за пределов периметра, так и между сегментами сети — должен быть защищён от перехвата и изменения передаваемых данных, а также от несанкционированного использования. Для этого необходимо применять шифрование каналов связи, строгую аутентификацию пользователей и контроль удалённых сессий.

Для реализации данной меры используются средства защиты информации, обеспечивающие безопасный удалённый доступ. Дополнительный уровень защиты обеспечивает многофакторная аутентификация.

УПД.14 Контроль доступа из внешних информационных (автоматизированных) систем

Мера предусматривает строгий контроль, фильтрацию и регистрацию всех попыток подключения к защищаемой системе — АСУ ТП — из-за пределов её периметра. К таким

подключениям относятся, например, соединения из корпоративной ИТ-сети, сети Интернет, а также подключения подрядчиков.

Для реализации меры применяются межсетевые экраны, аппаратные шлюзы и диоды данных, а также создаётся демилитаризованная зона (DMZ). Внешним системам запрещено подключаться напрямую к контроллерам и серверам АСУ ТП. Обмен данными осуществляется через шлюз или прокси-сервер, размещённый в DMZ. Он выступает единственным посредником и обеспечивает строгий контроль сетевых сессий.

KICS for Nodes

Мера реализуется в части:

- проверки входящего сетевого трафика на наличие действий, характерных для сетевых атак, а также блокирования сетевой активности со стороны атакующих устройств с помощью задачи «Защита от сетевых угроз»;
- отслеживания статуса работы и контроля работы брандмауэра Windows с помощью задачи «Управление сетевым экраном»;
- предотвращение несанкционированного сетевого доступа с помощью белых списков: запуск разрешён только доверенным приложениям, которым разрешено сетевое взаимодействие. Белые списки формирует компонент «контроль приложений».

KICS for Linux Nodes

Мера реализуется задачей «Управление сетевым экраном» в части осуществления контроля состояния встроенного меж сетевого экрана ОС и предотвращения несанкционированного изменения его конфигураций.

Мера реализуется также в части предотвращения несанкционированного сетевого доступа с помощью белых списков: запуск разрешён только доверенным приложениям, которым разрешено сетевое взаимодействие. Белые списки формирует компонент «контроль приложений».

KICS for Networks

Мера реализуется в части:

- мониторинг сетевых сессий, выявление неразрешённых сетевых сессий, в том числе с доступом из внешних информационных (автоматизированных) систем;
 - в режиме обучения формируется «белый список» разрешённых сетевых взаимодействий. Если внешняя система — например, сервер из ИТ-сети — пытается обратиться к внутреннему активу (ПЛК или HMI) с неавторизованного IP-адреса либо по неразрешённому протоколу, KICS for Networks немедленно регистрирует инцидент.
 - обнаружения вторжений в сессиях, в том числе с доступом из внешних информационных (автоматизированных) систем.
-

Revision #3

Created 21 September 2025 19:26:24 by Olga Sinotova

Updated 22 October 2026 12:29:37 by Olga Sinotova