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

УПД.0 Разработка политики управления доступом

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

УПД.1 Управление учетными записями пользователей

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

УПД.2 Реализация модели управления доступом

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».

УПД.3 Доверенная загрузка

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.

УПД.4 Разделение полномочий (ролей) пользователей

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

УПД.5 Назначение минимально необходимых прав и привилегий

Для реализации данной меры нужно разработать матрицу доступа, желательно в составе проектной документации на АСУ ТП.

УПД.6 Ограничение неуспешных попыток доступа в автоматизированную систему

KICS for Nodes

Мера реализуется для рабочих мест на базе ОС Windows в части обнаружения попыток подбора пароля путем анализа журналов событий Windows с помощью задачи «Анализ журналов».

УПД.7 Предупреждение пользователя при его доступе к информационным ресурсам

Для реализации данной меры используются встроенные механизмы защиты информации.

УПД.8 Оповещение пользователя при успешном входе о предыдущем доступе к автоматизированной системе

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».

УПД.9 Ограничение числа параллельных сеансов доступа

Для реализации данной меры используются встроенные механизмы защиты информации, а также данную меру можно реализовать с помощью служб каталогов LDAP или Microsoft AD.

УПД.10 Блокирование сеанса доступа пользователя при неактивности

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

УПД.11 Управление действиями пользователей до идентификации и аутентификации

Для реализации данной меры используются механизмы встроенной защиты информации и СЗИ от НСД.

УПД.12 Управление атрибутами безопасности

Для реализации данной меры используются встроенные механизмы защиты информации, а также данную меру можно реализовать с помощью служб каталогов LDAP или Microsoft AD.

УПД.13 Реализация защищенного удаленного доступа

Для реализации данной меры используются средства защиты информации для организации удалённого доступа.

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

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».

KICS for Linux Nodes

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

KICS for Networks

Мера реализуется в части:

- мониторинг сетевых сессий, выявление неразрешенных сетевых сессий, в том числе с доступом из внешних информационных (автоматизированных) систем;
- обнаружения вторжений в сессиях, в том числе с доступом из внешних информационных (автоматизированных) систем.

Revision #2
Created 21 September 2025 19:26:24 by Olga Sinotova
Updated 19 February 2026 13:38:23 by Olga Sinotova