

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

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

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

Для реализации данной меры выполняется разработка нормативных внутренних документов, регламентирующих правила пользования машинными носителями для сотрудников субъекта КИИ.

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

Требование реализуется посредством организационных мер, предусмотренных внутренними нормативными и распорядительными документами субъекта КИИ. В таких документах следует установить порядок учёта, выдачи, использования, хранения, перемещения и уничтожения носителей информации.

Все используемые в организации носители информации, в особенности съёмные, подлежат регистрации и инвентарному учёту. Для каждого носителя необходимо определить уникальный инвентарный номер, назначить ответственное лицо и, при необходимости, указать место хранения, категорию обрабатываемой информации и допущенных к работе пользователей. Следует также предусмотреть периодическую сверку фактического наличия носителей с учётными данными, порядок действий при их утрате или повреждении, а также контроль за безопасным удалением информации и выводом носителей из эксплуатации.

Также для меры предусмотрена техническая реализация. Частично она реализуется в виде использования:

KICS for Nodes

Мера реализуется в части контроля использования внешних USB-устройств и подключаемых по USB CD/DVD-дисководов, а также формированию перечня "Доверенных устройств" с помощью компонента «Контроль устройств».

При подключении устройства, доступ к которому запрещён, приложение блокирует доступ к нему для пользователей, указанных в соответствующем правиле, и отображает уведомление. При попытке чтения с устройства или записи на него приложение блокирует соответствующие операции для указанных в правиле пользователей без отображения уведомления.

KICS for Linux Nodes

Мера реализуется в части контроля использования внешних USB-устройств и подключаемых по USB CD/DVD-дисководов, а также формированию перечня "Доверенных устройств" с помощью компонента «Контроль устройств».

При подключении устройства, доступ к которому запрещён, приложение блокирует доступ к нему для пользователей, указанных в соответствующем правиле, и отображает уведомление. При попытке чтения с устройства или записи на него приложение блокирует соответствующие операции для указанных в правиле пользователей без отображения уведомления.

Kaspersky Security Center

Kaspersky Security Center предоставляет базовые возможности для учёта программного обеспечения и оборудования:

- Позволяет просматривать информацию о подключенных жестких дисках, носителях через отчеты и инвентаризацию;
- Позволяет настроить мониторинг подключенных носителей и генерации соответствующих событий;
- Позволяет настроить мониторинг подключения съемных носителей и генерации соответствующих событий;
- Позволяет настроить политики в KSC для ограничения использования съёмных носителей, если это необходимо.

Для реализации меры ЗНИ.1 KSC необходимо комбинировать с специализированными СЗИ (такими как Secret Net Studio или Dallas Lock) для полноценного учёта и контроля машинных носителей.

ЗНИ.2 Управление физическим доступом к машинным носителям информации

Для выполнения требования ЗНИ.2 необходим комплексный подход, включающий два взаимосвязанных и равноценных направления: организационные меры и физическая защита.

Организационные меры должны определять порядок обращения с носителями информации и ответственность сотрудников. В документах организации необходимо однозначно установить границы контролируемой зоны: например, указать, относится ли к ней серверная, отдельный этаж, здание или территория предприятия. Также следует определить порядок доступа в эту зону, назначить ответственных лиц и установить правила внесения, использования, хранения и выноса носителей.

Для контроля перемещения носителей необходимо вести журнал учёта. В нём рекомендуется фиксировать сведения о носителе, его владельце или ответственном лице, дате и времени перемещения, направлении перемещения (внос или вынос), цели и основании операции, а также данные сотрудника, разрешившего её. Порядок ведения и

хранения журнала должен быть закреплён во внутренних документах организации.

Физическая защита может включать средства контроля и управления доступом (СКУД), видеонаблюдение, охрану и устройства обнаружения несанкционированного выноса носителей, например детекторы на выходах из контролируемой зоны.

ЗНИ.3 **Необходимо комплексный подход, включающий два взаимосвязанных и равноценных направления: организационные меры и физическая защита.**

Для выполнения требования ЗНИ.3 необходим комплексный подход, включающий два взаимосвязанных и равноценных направления: организационные меры и физическая защита.

Организационные меры должны определять порядок обращения с носителями информации и ответственность сотрудников. В документах организации необходимо однозначно установить границы контролируемой зоны: например, указать, относится ли к ней серверная, отдельный этаж, здание или территория предприятия. Также следует определить порядок доступа в эту зону, назначить ответственных лиц и установить правила внесения, использования, хранения и выноса носителей.

Для контроля перемещения носителей необходимо вести журнал учёта. В нём рекомендуется фиксировать сведения о носителе, его владельце или ответственном лице, дате и времени перемещения, направлении перемещения (внос или вынос), цели и основании операции, а также данные сотрудника, разрешившего её. Порядок ведения и хранения журнала должен быть закреплён во внутренних документах организации.

Физическая защита может включать средства контроля и управления доступом (СКУД), видеонаблюдение, охрану и устройства обнаружения несанкционированного выноса носителей, например детекторы на выходах из контролируемой зоны.

ЗНИ.4 **Необходимо применять средства, обеспечивающие невозможность прочесть данные без соответствующего ключа. Для этого могут использоваться сертифицированные средства криптографической защиты информации (СКЗИ) либо специализированные USB-накопители с аппаратным шифрованием и аутентификацией по PIN-коду.**

Для выполнения данной меры необходимо применять средства, обеспечивающие невозможность прочесть данные без соответствующего ключа. Для этого могут использоваться сертифицированные средства криптографической защиты информации (СКЗИ) либо специализированные USB-накопители с аппаратным шифрованием и аутентификацией по PIN-коду.

В случае аппаратного шифрования расшифрование выполняется непосредственно внутри накопителя после ввода PIN-кода; в открытом виде данные не передаются за его пределы. При выборе решения следует убедиться, что оно соответствует применимым требованиям и имеет необходимые сертификаты. Рутокен и JaCarta могут использоваться в составе решения для хранения ключей или аутентификации, однако не всякая модель этих устройств является зашифрованным USB-накопителем.

ЗНИ.5 **Необходимо применять средства, обеспечивающие невозможность прочесть данные без соответствующего ключа. Для этого могут использоваться сертифицированные средства криптографической защиты информации (СКЗИ) либо специализированные USB-накопители с аппаратным шифрованием и аутентификацией по PIN-коду.**

Мера предусматривает контроль интерфейсов, через которые к защищаемой системе могут подключаться внешние устройства и носители информации. К таким интерфейсам относятся:

- USB-порты;
- COM-порты (последовательные порты);
- LPT-порты (параллельные порты);
- FireWire и Thunderbolt;
- Bluetooth-адаптеры;
- Wi-Fi-адаптеры;
- сетевые карты, в том числе внешние адаптеры, подключаемые через USB.

Цель меры — исключить возможность подключения несанкционированных устройств через доступные интерфейсы.

В Kaspersky Industrial CyberSecurity for Nodes (KICS for Nodes) мера реализуется в части контроля внешних устройств, подключаемых через USB:

- регистрация и контроль использования внешних USB-устройств, в том числе подключаемых по USB дисководов CD/DVD, с помощью задачи «Контроль устройств»;
- формирование списка разрешающих правил для подключения флеш-накопителей и других внешних устройств. Правила создаются на основе сведений операционной системы об устройствах, которые ранее подключались к защищаемому узлу, с помощью задачи «Формирование правил контроля устройств».

KICS for Linux Nodes

Мера реализуется в части:

- регистрации и контроля использования внешних USB-устройств и подключаемых по USB CD/DVD-дисководов с помощью задачи «Контроль устройств»;
- формирования списка разрешающих правил для подключения флеш-накопителей и других внешних устройств на основе данных операционной системы обо всех внешних устройствах, которые ранее подключались к защищаемому устройству, с помощью задачи «Формирование правил контроля устройств».

ЗНИ.6 Контроль ввода (вывода) информации на машинные носители

Для реализации данной меры используются средства контроля съемных носителей информации, а также физическое ограничение доступа к портам ввода-вывода.

ЗНИ.7 Контроль подключения машинных носителей информации

Мера предусматривает регистрацию и контроль факта подключения съемных носителей информации к защищаемому узлу, включая USB-флеш-накопители, внешние жесткие диски и SD-карты.

В KICS for Nodes мера реализуется с помощью следующих задач:

- «Контроль устройств» — для регистрации и контроля использования съемных носителей информации;
- «Формирование правил контроля устройств» — для создания списка разрешающих правил на основе сведений операционной системы о внешних устройствах, ранее подключавшихся к защищаемому узлу.

KICS for Linux Nodes

- «Контроль устройств» — для регистрации и контроля использования съемных носителей информации;
- «Формирование правил контроля устройств» — для создания списка разрешающих правил на основе сведений операционной системы о внешних устройствах, ранее подключавшихся к защищаемому узлу.

???8 ????????? (????????) ????????? ?? ????????? ????????? ?????????

Для реализации данной меры разрабатываются положения внутренних нормативных документов, регламентирующих правила уничтожения (стирания) информации на машинных носителях, а также СЗИ от НСД с функцией уничтожения информации.