Crosstech Endpoint Device Management

Руководство пользователя
Часть 2
Сценарии задач

CCEDM Release 8.0.0

АННОТАЦИЯ

Данный документ входит в состав руководства пользователя для работы в Системой Crosstech Endpoint Device Management (далее – CEDM).

Руководство содержит сведения, необходимые для настройки сценариев задач для устройств под управлением операционных систем (ОС) Windows, macOS или Linux.

СОДЕРЖАНИЕ

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Определение
Ansible	Ansible – система управления конфигурациями, написанная на языке программирования Python, с использованием декларативного языка разметки для описания конфигураций. Применяется для автоматизации настройки и развертывания программного обеспечения
Crosstech Endpoint Device Management (CEDM)	Система централизованного мониторинга и управления рабочими станциями и серверам
Universally unique identifier (UUID)	Всемирно уникальный идентификатор
Аварийная ситуация	Опасное техногенное происшествие, создающее на объекте, определенной территории или акватории угрозу жизни и здоровью людей и приводящее к разрушению или повреждению зданий, сооружений, оборудования и транспортных средств, нарушению производственного или транспортного процесса, нанесению ущерба окружающей среде [Федеральный закон от 30 декабря 2009 года N 384-ФЗ «Технический регламент о безопасности зданий и сооружений»]
Автоматизированное рабочее место (АРМ)	Программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида. Объединяет программно-аппаратные средства, обеспечивающие взаимодействие человека с компьютером
Авторизация	Процесс принятия решения о предоставлении доступа пользователю на выполнение операции на основании каких-либо знаний о нем. К этому моменту пользователь уже должен быть идентифицирован и аутентифицирован (подтверждена его идентичность)
Администратор доступа	Администратор подсистемы ПАА, осуществляющий настройку конфигурации Системы, а также создание, удаление и редактирование профилей пользователей CEDM
Аутентификация	Процедура проверки подлинности пользователя при попытке получить доступ к информационной системе
Задача в Системе CEDM	Действие или последовательность действий, которые инициируются администратором в веб-интерфейсе

	сервера CEDM и выполняются удаленно на выбранных агентах (АРМ)
Кратковременный сбой	Ненормальный режим, представляет собой состояние, характеризуемое неспособностью выполнить необходимую функцию, исключая неспособность, возникающую во время профилактических работ или других плановых мероприятий, либо в результате недостатка внешних ресурсов
Логин пользователя	Уникальный идентификатор учетной записи CEDM Server, необходимый для авторизации пользователя в системе
Оконечное устройство	АРМ или УРМ
Подсистема аутентификация и авторизации (ПАА)	Подсистема CEDM, предназначенная для управления конфигурацией и пользователями Системы
Профиль конфигурации	Набор предопределенных параметров и настроек, который определяет эталонное состояние оконечного устройства в Системе CEDM. Профиль конфигурации включает в себя: • настройки операционной системы (ОС), такие как параметры безопасности, сетевые настройки и системные конфигурации; • политики безопасности, включая настройки firewall, антивирусного ПО и других средств защиты информации; • перечень программного обеспечения (ПО) с указанием требуемых версий; • список необходимых обновлений (патчей) ОС
Система управления рабочими станциями (СУРС)	Система CEDM, предназначенная для управления удаленными устройствами, проведения инвентаризации, также выполнения задач на устройствах
Пользователь CEDM	Пользователь Системы управления рабочими местами, выполняющий функции в соответствии с назначенной ему ролью
Роль	Перечень функциональных возможностей, доступных пользователю CEDM
Сценарий задачи	Описание последовательности действий на языке YAML для выполнения какой-либо задачи автоматизации без привязки к конкретным артефактам или оконечным устройствам

Сценарий задачи стандартный	Сценарий задачи доступный всем пользователям Системы. То есть не имеющий разделения доступа на основе групп
Сценарий задачи групповой	Сценарий задачи, который привязан к определенной группе устройств. Задачи на его основе могут выполняться только на устройствах, входящих в указанную в сценарии группу. К сценарию имеют доступ только те пользователи, которые имеют доступ к группе, указанной в сценарии
Сценарий задачи системный	Сценарий задачи, который входит в поставку с Системой
УРМ	Удаленное рабочее место или удаленное устройство
Учетная запись	Хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания и предоставления доступа к его личным данным и настройкам

2. ОБЩИЕ СВЕДЕНИЯ О СЦЕНАРИЯХ В СИСТЕМЕ CEDM

Схемы сценариев в CEDM представляют собой набор инструкций для выполнения определенных задач на удаленных устройствах.

2.1. Компоненты схемы сценариев в Системе CEDM

В Системе CEDM схема сценария содержит архив, включающий четыре файла: «hosts», «role.yaml», «config.json» и «run.sh».

Вместе эти файлы образуют плейбук Ansible. Основой сценария является плейбук на языке YAML.

2.1.1. Файл «hosts»

В файле «hosts» определяются целевые хосты, переменные и параметры подключения для выполнения задач Ansible на удаленных устройствах. В системе CEDM файлы «hosts» имеют типовую структуру в зависимости от семейства ОС целевого устройства: Windows или Linux. Таким образом, при разработке новой схемы сценария задачи можно использовать типовой файл «hosts».

Ниже представлен пример содержимого файла «hosts» для выполнения задач на устройствах под управлением ОС Windows:

Содержимое файла «hosts»

```
[windows]
win_host1

[windows:vars]
ansible_connection=ssh
ansible_shell_type=cmd
ansible_ssh_common_args=-o StrictHostKeyChecking=no -o
UserKnownHostsFile=/dev/null
ansible_ssh_retries=1
ansible_ssh_timeout=5
ansible_become_method=runas
ansible_ssh_transfer_method=scp
ansible_scp_extra_args=-O
```

где:

- [windows] – имя группы целевых хостов для выполнения задачи;

- win_host1 – идентификатор или запись типа «ALIAS» целевого хоста в группе «windows». Система CEDM автоматически передает идентификатор (запись типа «ALIAS») целевого хоста в сценарий;
- [windows:vars] – это секция, определяющая переменные и параметры подключения, которые будут применяться ко всем хостам в группе «windows».

2.1.2. Файл «role.yaml»

Файл «role.yaml» – плейбук (playbook), используемый Ansible для управления оконечным устройством, написанный на языке YAML. Содержит последовательность задач, которые требуется выполнить на целевых хостах.

Ниже представлен пример содержимого файла «role.yaml»:

Содержимое файла «yaml»

```
--- #начало YAML-документа
hosts: all #определяет целевые хосты выполняемых задач
  gather_facts: no #определяет, будет ли Ansible собирать информацию о целевой системе (IP-адреса, тип ОС, объем памяти и т. д.) перед выполнением задач
  vars: #в блоке определяются переменные, используемые в плейбуке
      version: '1.2'
      path: 'C:\Program Files (X86)\Kaspersky Lab\'
  tasks: #в блоке определяется перечень выполняемых задач
    - name: Check_folder #поле для указания имени задачи
      win_stat: #модуль Ansible, используемый в задаче
        path: 'C:\ProgramData\CEDM\desktopagent\cache'
      register: folder_stat #результат выполнения задачи будет сохранен в переменную «folder_stat»
      async: 1 #параметр определяет, должна ли задача выполняться асинхронно. Позволяет запускать длительные операции в фоновом режиме, не блокируя выполнение остальных задач
      poll: 0 #параметр используется в сочетании с «async» для определения частоты проверки статуса асинхронной задачи. Указывается интервал в секундах между проверками статуса. Значение 0 означает «запустить и забыть»
      when: product_id == "scan" #параметр определяет условия выполнения задачи
```

2.1.3. Файл «config.json»

Структура и параметры сценария определяются с помощью файла конфигурации «config.json», который:

- содержит описание структуры сценария:
- определяет ОС, для которой предназначен сценарий;
- содержит многоязычное описание сценария для отображения в пользовательском интерфейсе;
- задает полный перечень параметров сценария с их типами и свойствами.

Поддерживаются следующие типы параметров:

- FILE – файл;
- STRING – строка;
- LIST – выпадающий список;
- INVENTORY – значения из инвентаризации.

В файле «config.json» определяется место заполнения каждого параметра (в шаблоне или в задаче), а также настраиваются зависимости между параметрами и условия их отображения.

В файле «config.json» контролируется корректность заполнения параметров, определяется обязательность параметров и их ограничения.

Ниже представлен пример содержимого файла «config.json»:

```bash
{
    "description": {
        "RU": "Доставляет файл на ОС: Windows",
        "EN": "Delivers the file to OS: Windows"
    },
    "operating_system": "WINDOWS",
    "parameters": [
        {
            "type": "FILE",
            "ui_name": {
                "RU": "Файл",
                "EN": "File"
            },
            "parameter_name": "f",
            "is_nullable": false,
            "place_of_filling": "TEMPLATE",
            "is_password": false,
```

```
            "comment": {},
            "file_type": "",
            "parent_parameter_name": "",
            "list": [],
            "inventory_type": "",
            "field_code_for_filter": "",
            "field_code_for_selecting_value": ""
        },
        {
            "type": "STRING",
            "ui_name": {
                "RU": "Путь на конечном устройстве",
                "EN": "Filepath on the client device"
            },
            "parameter_name": "m",
            "is_nullable": false,
            "place_of_filling": "TEMPLATE",
            "is_password": false,
            "comment": {"RU":"Укажите полный путь к каталогу, в
который необходимо доставить файл",
                        "EN":"Specify the full path to the
directory to which the file needs to be delivered"},
            "file_type": "",
            "parent_parameter_name": "",
            "list": [],
            "inventory_type": "",
            "field_code_for_filter": "",
            "field_code_for_selecting_value": ""
        },
        {
            "type": "STRING",
            "ui_name": {
                "RU": "Имя файла без расширения",
                "EN": "File name without extension"
            },
            "parameter_name": "n",
            "is_nullable": true,
            "place_of_filling": "TEMPLATE",
            "is_password": false,
            "comment": {"RU":"Укажите имя файла без расширения,
в противном случае будет задано имя по умолчанию",
```

```
                        "EN":"Specify the file name without
extension, otherwise, a default name will be assigned"},
            "file_type": "",
            "parent_parameter_name": "",
            "list": [],
            "inventory_type": "",
            "field_code_for_filter": "",
            "field_code_for_selecting_value": ""
        }

    ]
}
```

2.1.4. Файл «run.sh»

Файл «run.sh» представляет собой bash-скрипт, который используется для запуска плейбука Ansible с необходимыми параметрами, в том числе параметрами, заданными в файле «config.json».

Ниже представлен пример содержимого файла «run.sh»:

```bash
#!/bin/bash #Шебанг, указывающий что это bash-скрипт
#Обработка аргументов командной строки
while getopts u:a:p:i:m:n:f:z: flag
do
    case "${flag}" in
#Каждый флаг соответствует определенному параметру
        u) var_user=${OPTARG};; #u: пользователь
        a) var_ip=${OPTARG};; #a: IP-адрес
        p) var_port=${OPTARG};; #p: порт
        m) var_arguments=${OPTARG};; #i: файл ключа
        i) var_key_file=${OPTARG};; #m: аргументы
        f) var_file_path=${OPTARG};; #f: путь к файлу
        z) var_product_id=${OPTARG};; #z: идентификатор
продукта
    esac
done
# установка значений по умолчанию
var_port=${var_port:-22}
var_user=${var_user:-"system"}
# вывод значений переменных
```

```
echo $var_user;
echo $var_ip;
echo $var_port;
echo $var_key_file;
echo $var_path;
echo $var_file_name;
echo $var_file_path;
echo $var_product_id;
#Меняет текущий рабочий каталог на тот, в котором находится скрипт
cd "$(dirname "$0")"
#Запуск плейбука Ansible с полученными выше аргументами
ansible-playbook role.yaml -vvv -i ./hosts -l win_host1 --extra-vars "path=$var_path" --extra-vars "file_name=$var_file_name" --extra-vars "ansible_host=$var_ip" --extra-vars "ansible_port=$var_port"  --extra-vars "ansible_user=$var_user" --extra-vars "file_path=$var_file_path" --extra-vars "product_id=$var_product_id" --private-key $var_key_file
```

2.2. Загрузка файлов в Систему

При настройке параметров некоторых сценариев требуется выбора файлов (например, bat-скрипты, файлы сертификатов и т. д.). Необходимые файлы должны быть загружены в Систему перед настройкой самого сценария. Файлы загружаются в Систему через раздел веб-интерфейса «Администрирование» → «Хранилище файлов».

2.3. Категории сценариев

Все сценарии распределены на категории. Каждой категории соответствует определенный префикс, который используется в кодах сценариев. Подробная информация о категориях представлена в таблице 1.

Таблица 1. Категории сценариев

№	Категории	Префикс
1	Управление безопасностью (Security Management)	SEC_MGMT
2	Управление системными настройками и конфигурацией (System Configuration Management)	SYS
3	Управление программным обеспечением (Software Management)	SFT
4	Управление локальными политиками и доступом (Local Policy & Access Management)	POL
5	Выполнение скриптов и произвольных команд (Scripting & Execution)	SE

2.4. Общие параметры сценариев

У некоторых сценариев, независимо от того, для какой операционной системы они предназначены, есть общие параметры, заполняемые при создании задачи.

Таким общим параметром является «Журнал выполнения задач шаблона» – данный параметр определяет необходимость отображения пропущенных задач в журнале выполнения:

- «Да» – пропущенные задачи будут отображены в журнале выполнения задач шаблона;
- «Нет» – пропущенные задачи не будут отображены в журнале выполнения задач шаблона. Является значением по умолчанию.

2.5. Параметры, необходимые для установки программного обеспечения в тихом режиме

При выполнении на операционной системе Windows сценария «Установка программного обеспечения» можно использовать специальные параметры, чтобы взаимодействовать с программой или установщиком программы без участия пользователя и устанавливать программного обеспечение в тихом режиме. Параметры задаются с помощью ключей, которые необходимо указать в шаблоне в поле «Параметры запуска». В таблице 2

представлен перечень параметров и соответствующих им ключей для трех типов установщиков.

Таблица 2. Параметры запуска

Параметр	**Инсталлятор NSIS**	**Инсталлятор Inno setup**	**MSI-установщики**
Обычная установка	без параметров	без параметров	msiexec /i
Только прогресс-бар при установке (Quiet-режим)	/S	/SILENT	/qb
Полностью скрытая установка (Silent-режим)		/VERYSILENT	/qn
Обычная деинсталляция	без параметров	без параметров	msiexec /x
Только прогресс-бар при деинсталляции (Quiet-режим)	/S	/SILENT	/qb
Полностью скрытая деинсталляция (Silent-режим)		/VERYSILENT	/qn

3. СЦЕНАРИИ ДЛЯ ОС WINDOWS

3.1. Управление политиками PowerShell

Код: SE_PWSH_POLICY

Сценарий предназначен для настройки политик выполнения скриптов PowerShell на оконечных устройствах под управлением ОС Windows. Позволяет централизованно управлять уровнями безопасности выполнения скриптов для различных областей действия.

3.1.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 3.

Таблица 3. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Область действия	В шаблоне	Область влияния политики выполнения. Выбирается один из двух вариантов: • «CurrentUser» – политика выполнения влияет только на текущего пользователя; • «LocalMachine» – политика выполнения влияет на всех пользователей на текущем компьютере	Да
Имя пользователя	В шаблоне	Поле доступно для заполнения только при выборе варианта «CurrentUser» в параметре «Область действия». Указывается имя пользователя (sAMAccountName), на которого будет влиять политика выполнения	Да
Политика выполнения	В шаблоне	Выбор политики из следующего перечня: • «AllSigned» – требует наличие подписи доверенного издателя для всех скриптов и файлов конфигурации, включая скрипты, подготовленные на локальном компьютере;	Да

		• «Bypass» – ничего не блокируется, никакие предупреждения и запросы не появляются; • «Default» – политика выполнения задается по умолчанию; • «RemoteSigned» – требует подпись доверенного издателя скриптов, скачанных из сети Интернет. Не требуется для локальных скриптов; • «Restricted» – запрещает выполнение всех файлов скриптов, включая следующие форматы: PS1XML, PSM1, PS1; • «Undefined» – в текущей области не задана политика выполнения; • «Unrestricted» – допускает выполнение неподписанных скриптов. Существует риск запуска вредоносных сценариев	

Важно: политика выполнения не является системой безопасности, ограничивающей действия локальных пользователей. Пользователи могут обойти ограничения, введя содержимое скрипта непосредственно в командной строке.

3.2. Управление контролем учетных записей

Код: SEC_MGMT_UAC

Сценарий предназначен для централизованного управления настройками User Account Control (UAC) на оконечных устройствах под управлением ОС Windows. UAC — это функция безопасности, которая ограничивает возможности выполнения вредоносного кода с привилегиями администратора.

3.2.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 4.

Таблица 4. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность

Уровень UAC	В шаблоне	В параметре необходимо выбрать один из четырех уровней уведомлений: • «Всегда уведомлять» – соответствует 4 уровню. Максимальный уровень безопасности с полным контролем; • «Уведомлять меня (по умолчанию)» – соответствует 3 уровню. Получение уведомлений только при попытках приложений внести изменения (по умолчанию); • «Уведомлять меня (не затемнять рабочий стол)» – соответствует 2 уровню. Получение уведомлений только при попытках приложений внести изменения (не затемнять рабочий стол); • «Никогда не уведомлять» – соответствует 1 уровню. Отключение всех уведомлений UAC	Да

3.3. Управление паролями локальных пользователей

Код: SEC_MGMT_PASS

Сценарий предназначен для централизованного изменения паролей локальных учетных записей пользователей Windows на оконечных устройствах. Позволяет устанавливать новые пароли с возможностью принудительной смены при следующем входе в систему.

3.3.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 5.

Таблица 5. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность

Имя пользователя	В задаче	Имя учетной записи пользователя	Да
Пароль	В задаче	Пароль учетной записи пользователя. При вводе будет скрыт звездочками	Да
Требовать смены пароля при следующем входе в систему?	В задаче	Необходимость смены пароля после первого входа в Систему. Выбирается один из двух вариантов: • «Да» – пароль требуется сменить после первого входа в Систему; • «Нет» – смена пароля не требуется	Да

3.4. Управление профилями Cisco AnyConnect

Код: SFT_MGMT_CISCO_AC

Сценарий предназначен для централизованного управления профилями VPN-подключений Cisco AnyConnect Secure Mobility Client на оконечных устройствах с ОС macOS. Позволяет добавлять и удалять XML-профили конфигурации с автоматической перезагрузкой служб.

3.4.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 6.

Таблица 6. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Файл профиля VPN Cisco AnyConnect	В шаблоне	Поле для загрузки XML-файла с данными профиля VPN Cisco AnyConnect	Нет
Действие	В шаблоне	Выбор необходимого действия с профилем. Выбирается один из двух вариантов: • «Добавить профиль» – необходимость добавления файла профиля; • «Удалить профиль» – необходимость удаления файла профиля	Да

Имя VPN профиля	В шаблоне	Поле для указания имени VPN-профиля. Указывается имя файла без расширения	Да

3.4.2. Примеры использования

3.4.2.1. Добавление корпоративного VPN-профиля

Действие в шаблоне: «Добавить профиль»
Файл профиля: corporate_vpn.xml
Имя VPN профиля: corporate_vpn
Результат:

- профиль добавлен в *C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\corporate_vpn.xml*;
- службы vpnagent и aciseagent перезагружены.

3.4.2.2. Удаление устаревшего профиля

Действие в шаблоне: «Удалить профиль»
Файл профиля: не требуется
Имя VPN профиля: «old_vpn_config»
Результат:

- файл «old_vpn_config.xml» удален из директории профилей;
- службы перезагружены.

Примечания:

1) После выполнения задачи необходимо вручную запустить агента Cisco Anyconnect, выбрать доставленный профиль из списка и нажать кнопку «Connect».
2) Для успешной доставки или удаления профиля настроек агента Cisco Anyconnect необходимо указать тайм-аут выполнения задачи не менее 60 секунд.

3.4.2.3. Требования к XML-профилям

XML-файл профиля должен соответствовать схеме Cisco AnyConnect. Пример содержимого профиля:

```xml
<?xml version="1.0" encoding="UTF-8"?>
```

```
<AnyConnectProfile
xmlns="http://schemas.xmlsoap.org/vpn/profile/2007">
    <ClientInitialization>
        <UseStartBeforeLogon
UserControllable="false">false</UseStartBeforeLogon>
        <AutomaticCertSelection
UserControllable="false">true</AutomaticCertSelection>
        <!-- Дополнительные настройки -->
    </ClientInitialization>
    <ServerList>
        <HostEntry>
            <HostName>vpn.company.com</HostName>
            <HostAddress>192.168.1.1</HostAddress>
        </HostEntry>
    </ServerList>
</AnyConnectProfile>
```

3.5. Управление профилями КриптоПро Ngate

Код: SFT_MGMT_NGATE

Сценарий предназначен для централизованного управления агентом КриптоПро NGate на оконечных устройствах под управлением ОС Windows. Позволяет настраивать параметры подключения к шлюзу и сертификаты безопасности через изменение ключей реестра ОС Windows для всех пользователей оконечного устройства.

3.5.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 7.

Таблица 7. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Настраиваемое значение	В шаблоне	Поле для выбора настраиваемого значения. Выбирается один из следующих вариантов: • «Адрес шлюза» – для всех локальных пользователей будет изменен адрес шлюза подключения; • «Сертификат» – для всех локальных пользователей будет	Да

		изменен сертификат подключения; • «Адрес шлюза и сертификат» – для всех локальных пользователей будут изменены адрес шлюза и сертификат подключения	
Адрес шлюза	В шаблоне	Поле для указания IP-адреса шлюза или FQDN. Например: • http://gateway.company.local • http://192.168.1.100	Нет
Отпечаток сертификата	В шаблоне	Поле для указания отпечатка сертификата в шестнадцатеричном формате. Например: a1b2c3d4e5f6g7h8i9j0	Нет

3.5.2. Примеры использования

3.5.2.1. Настройка адреса шлюза

Настраиваемое значение: Адрес шлюза
Адрес шлюза: gate.company.ru
Отпечаток сертификата: не требуется
Результат: для всех активных пользователей будет установлен адрес шлюза gate.company.ru.

3.5.2.2. Установка сертификата

Настраиваемое значение: Сертификат
Адрес шлюза: не требуется
Отпечаток сертификата: *1234567890ABCDEF12345EF12345678*
Результат: для всех активных пользователей будет установлен отпечаток сертификата.

3.5.2.3. Полная настройка подключения

Настраиваемое значение: Адрес шлюза и сертификат
Адрес шлюза: 192.168.1.100
Отпечаток сертификата: 1234567890ABCDEF12345EF12345678
Результат: полная конфигурация подключения для всех пользователей.

3.6. Установка Ivanti IDC

Код: SFT_INSTALL_IDC

Сценарий предназначен для автоматической установки программного обеспечения Ivanti Device and Application Control (IDC) на оконечных устройствах под управлением ОС Windows.

3.6.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 8.

Таблица 8. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Установочный архив Ivanti IDC	В шаблоне	Поле для выбора ZIP-архива с установочными файлами Ivanti IDC, содержащего клиентскую часть программы и необходимые компоненты для установки, а именно: • Client.exe – основной установочный файл клиентской части; • Client.x64.mst – MST-трансформация для 64-битной версии Windows; • дополнительные файлы конфигурации и библиотеки, необходимые для работы IDC	Да

3.7. Управление настройками Ivanti Device Control

Код: SFT_MGMT_IVANTI

Сценарий предназначен для управления Ivanti Device Control. Позволяет централизованно загружать политики безопасности и временные разрешения на оконечные устройства.

3.7.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 9.

Таблица 9. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Файл	В шаблоне	Поле для выбора файла с настройками. Допускается загрузка файлов формата DAT и MST	Нет

Выбор типа загружаемого файла	В шаблоне	Выбор типа загружаемой сущности. Выбирается один из двух вариантов: • «Политика»; • «Тикет»	Да

3.7.2. Примеры использования

3.7.2.1. Развертывание новой политики

Загружаем: «Политика»
Файл: Security_Policy_v2.mst
Результат: политика размещена в *C:\Program Files\Ivanti\Device and Application Control\Import\Security_Policy_v2.mst*

3.7.2.2. Временная приостановка IDC

Загружаем: «Тикет»
Файл: Emergency_Disable.dat
Результат: тикет активирован через размещение в *C:\Program Files\Ivanti\Device and Application Control\Ticket\ Emergency_Disable.dat*

3.8. Установка SSL\TLS сертификатов

Код: SEC_MGMT_CERT

Сценарий предназначен для централизованной установки SSL\TLS сертификатов в хранилища ОС Windows на оконечных устройствах. Позволяет автоматически развертывать корневые сертификаты, промежуточные сертификаты центров сертификации и пользовательские сертификаты в соответствующие системные хранилища.

3.8.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 10.

Таблица 10. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Файл сертификата	В шаблоне	Поле для выбора файла с сертификатами. Допускается загрузка файлов формата DER, CRT, CER и PEM	Нет
Хранилище сертификатов	В шаблоне	Поле для выбора хранилища сертификатов. Выбирается одно из следующих значений: • «AddressBook» – другие пользователи;	Да

		• «AuthRoot» – сторонние корневые центры сертификации; • «CertificateAuthority» – промежуточные центры сертификации; • «Disallowed» – сертификаты без доверия; • «My» – личное; • «Root» – доверенные корневые центры сертификации; • «TrustedPeople» – доверенные лица; • «TrustedPublisher» – доверенные издатели	

3.8.2. Примеры использования

3.8.2.1. Установка корневого центра сертификации организации

Файл сертификата: Company-Root-CA.cer

Хранилище сертификатов: Доверенные корневые центры сертификации

Результат: корневой сертификат организации установлен в системное хранилище Root, обеспечивая доверие к внутренним сертификатам.

3.9. Установка программного обеспечения

Код: SFT_INSTALL

Сценарий предназначен для централизованной установки программного обеспечения на оконечных устройствах с ОС Windows. Поддерживает установку MSI-пакетов и EXE-инсталляторов с гибкими настройками идентификации продуктов и параметров командной строки.

3.9.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 11.

Таблица 11. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность

Установочный файл	В шаблоне	Поле для выбора установочного файла. Допускается загрузка файлов формата EXE и MSI	Нет
Режим определения идентификатора продукта	В шаблоне	Поле для выбора режима определения идентификатора продукта: • «Авто» – задается, если у продукта нет идентификатора (ID) или он неизвестен. Для MSI необходимо получить ID из пакета, для EXE – использовать значение 0; • «Задать идентификатор» – задается для ручного указания GUID продукта	Да
ID продукта	В шаблоне	Поле для указания идентификатора продукта. Задается только при выборе режима «Задать идентификатор». Указывается в следующем формате: *{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}* Примечание: подробнее см. подразделе 7.1 документа «Руководство пользователя CEDM Server ч.1 – Управление системой»	Нет
Параметры запуска	В шаблоне	Поле для указания дополнительных аргументов командной строки	Нет
Путь к установочному файлу на оконечном устройстве	В шаблоне	Поле для указания пути к файлу. Необходимо указать для возможности запуска установочного файла, который уже находится на оконечном устройстве	Нет

3.9.2. Режимы работы и примеры

3.9.2.1. Режим 1: Загрузка и автоматическая установка MSI

ID продукта (режим): Авто
Установочный файл: 7-zip.msi

3.9.2.2. Режим 2: Установка EXE с указанным GUID

ID продукта (режим): «Задать идентификатор»
Установочный файл: TeamViewer.exe
ID продукта: {AC76BA86-1033-FFFF-7760-000000000006}
Параметры запуска: /S /v/qn

3.9.2.3. Режим 3: Установка с удаленного устройства

ID продукта (режим): Авто;

Запустить инсталлятор на удаленном устройстве: C:\Install\Software\AutoCAD2024.msi

Параметры запуска: INSTALLDIR="C:\AutoCAD" /quiet

3.9.2.4. Режим 4: Корпоративная установка с настройками

ID продукта (режим): «Задать идентификатор»

Установочный файл: Adobe_Acrobat_DC.exe

ID продукта (значение): {AC76BA86-1033-FFFF-7760-000000000006}

Параметры запуска: --silent --install-path="C:\Adobe"

3.10. Запуск скриптов

Код: SE_SCRIPT

Сценарий предназначен для централизованного выполнения PowerShell (.ps1) и пакетных (.bat/.cmd) скриптов на оконечных устройствах с ОС Windows. Поддерживает передачу аргументов командной строки и обеспечивает безопасное выполнение в изолированной рабочей среде.

3.10.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 12.

Таблица 12. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Файл скрипта	В шаблоне	Поле для выбора файла скрипта из списка. Поддерживаются файлы формата PS1, BAT и CMD	Да
Аргументы запуска скрипта	В шаблоне	Поле для указания ключей запуска скриптов	Нет

3.10.2. Примеры использования

3.10.2.1. Скрипт установки параметров IP-адреса и маски подсети

«Файл»: set-network.ps1

«Аргументы запуска скрипта»: -ip 192.168.1.100 -mask 255.255.255.0

Примечания:

1) При использовании строк с пробелами в аргументах рекомендуется заключать их в кавычки.
2) Аргументы передаются в том же виде, как если бы скрипт запускался из командной строки.
3) Синтаксис аргументов должен соответствовать ожиданиям скрипта.
4) При передаче путей в качестве аргументов рекомендуется использовать полные пути.

3.11. Доставка файла

Код: SE_FILE

Сценарий предназначен для централизованной доставки файлов на оконечные устройства под управлением ОС Windows. Позволяет копировать файлы в указанный каталог с возможностью переименования и автоматическим созданием необходимых директорий.

3.11.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 13.

Таблица 13. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Файл	В шаблоне	Поле для выбора файла, который будет доставлен на оконечные устройства	Да
Путь на оконечном устройстве	В шаблоне	Поле для указания пути на оконечном устройстве. Задается в формате: c:\\temp\\destination_dir	Да
Имя файла без расширения	В шаблоне	Поле для указания имени файла без расширения. Поле можно оставить пустым. В этом случае будет задано имя по умолчанию	Нет

3.12. Управление настройками брандмауэра Windows

Код: SEC_MGMT_FW

Сценарий предназначен для централизованного управления встроенным брандмауэром ОС Windows на оконечных устройствах. Позволяет настраивать основные параметры брандмауэра,

управлять правилами и профилями безопасности, включая создание пользовательских правил фильтрации трафика.

3.12.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 14.

Таблица 14. Состав и описание параметров сценария

Название параметра	**Место заполнения**	**Описание**	**Обязательность**
Действие	В шаблоне	Поле для выбора действий с брандмауэром: • «Включение брандмауэра» – активирует защиту брандмауэра; • «Отключение брандмауэра» – деактивирует защиту брандмауэра; • «Блокировать входящие соединения» – запрещает входящий трафик по умолчанию; • «Разрешить входящие соединения» – разрешает входящий трафик по умолчанию; • «Блокировать исходящие соединения» – запрещает исходящий трафик по умолчанию; • «Разрешить исходящие соединения» – разрешает исходящий трафик по умолчанию; • «Разрешить ICMP v4 (ping)» – включает поддержку ping-запросов; • «Добавить правило в брандмауэр» – создает новое правило фильтрации; • «Отключить правило в брандмауэре» – удаляет существующее правило Примечание: для действий «Отключить правило в брандмауэре» и «Добавить правило в брандмауэр» необходимо	Да

		заполнить значения всех параметров. Для всех остальных действий указать только профиль брэндмауэра	
Профиль брэндмауэра	В шаблоне	Поле для выбора действий с брандмауэром: • «Доменный профиль» – применяется в корпоративных доменных сетях; • «Частный профиль» – используется в домашних и частных сетях; • «Публичный профиль» – применяется для общественных и недоверенных сетей; • «Все профили» – применяется настройки всех профилей одновременно	Нет
Имя правила	В шаблоне	Поле для указания имени правила, которое используется для добавления или отключения правила	Нет
Порт	В шаблоне	Поле для указания номера порта или диапазона портов в правиле. Например: 8080 или 443-450	Нет
Действие правила	В шаблоне	Поле для выбора типа действия для правила. Выбирается один из двух вариантов: • «Разрешить»; • «Запретить»	Нет
Направление трафика	В шаблоне	Поле для выбора типа направления трафика для правила. Выбирается один из двух вариантов: • «Входящий трафик»; • «Исходящий трафик»	Нет
Тип протокола	В шаблоне	Поле для выбора типа протокола: • «TCP протокол Transmission Control Protocol»; • «UDP протокол»; • «Протокол ICMPv4»; • «Протокол ICMPv6»	Нет

3.12.2. Примеры использования

3.12.2.1. Включение брандмауэра для домашней сети

Действие: «Включение брандмауэра»

Профиль брандмауэра: Частный профиль
Результат: активация защиты для частных сетей с настройками по умолчанию.

3.12.2.2. Блокировка входящего трафика в публичных сетях

Действие: «Блокировать входящие соединения»
Профиль брандмауэра: Публичный профиль
Результат: запрет всех входящих соединений в общественных сетях.

3.12.2.3. Разрешение ping-запросов для всех сетей

Действие: «Разрешить ICMP v4 (ping)»
Профиль брандмауэра: Все профили
Результат: включение поддержки ping во всех сетевых профилях.

3.12.2.4. Создание правила для веб-сервера

Действие: «Добавить правило в брандмауэр»
Профиль брандмауэра: Доменный профиль
Имя правила: Web Server HTTP
Порт: 80
Действие правила: «Разрешить»
Направление трафика: Входящий трафик
Тип протокола: TCP протокол
Результат: создание правила для разрешения HTTP-трафика на порт 80.

3.12.2.5. Настройка диапазона портов для FTP

Действие: «Добавить правило в брандмауэр»
Имя правила: FTP Passive Ports
Порт: 20000-20100
Действие правила: «Разрешить»
Направление трафика: Входящий трафик
Тип протокола: TCP протокол
Результат: разрешение FTP passive mode через диапазон портов.

3.13. Настройка локальных политик безопасности

Код: POL_MGMT_LGP

Сценарий предназначен для централизованного управления локальными политиками безопасности ОС Windows на оконечных устройствах. Позволяет настраивать политики паролей, аудита и права пользователей.

3.13.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 15.

Таблица 15. Состав и описание параметров сценария

Название параметра	**Место заполнения**	**Описание**	**Обязательность**
Файл шаблона политик безопасности	В шаблоне	Поле для выбора файла шаблона политик безопасности для применения готовой конфигурации. Поддерживаются файлы формата CFG и INF	Нет
Действия	В шаблоне	Поле для выбора необходимых действий: • «Предустановленные настройки» – настраивает локальные групповые политики согласно предопределенным значениям; • «Настройка парольной политики» – позволяет настроить одно значение из парольной политики; • «Настройка аудита событий» – позволяет настроить одно значение политик аудита событий; • «Настройка привилегированных прав» – позволяет настроить одно значение привилегированных прав; • «Настройка политик безопасности согласно шаблону» – позволяет загрузить файл шаблона политик безопасности; • «Настройка расширенных политик аудита» – позволяет настроить одно значение расширенных политик аудита	Да

Настраиваемое значение	В шаблоне	Поле для выбора настраиваемого значения, зависящего от выбранного действия (подробное описание представлено ниже после таблицы)	Нет
Значение	В шаблоне	Поле для указания нового значения для выбранного параметра	Нет
Отображение пропущенных задач	В задаче	Необходимость отображения пропущенных задач. Выбирается один из двух вариантов: • «Да» – пропущенные задачи будут отображены; • «Нет» – пропущенные задачи не будут отображены. Данное значение является значением по умолчанию	Нет

Ниже представлен список настраиваемых значений в зависимости от выбранного действия:

1) «Предустановленные настройки» – нет настраиваемых значений.
2) «Настройка парольной политики»:
   - «Максимальный срок действия пароля (в днях)» (MaximumPasswordAge) – указывается максимальный возраст пароля (в днях);
   - «Минимимальной срок действия пароля (в днях)» (MinimumPasswordAge) – указывается минимальный возраст пароля (в днях);
   - «Минимальная длина пароля» (MinimumPasswordLength);
   - «Требовать использование сложного пароля» (PasswordComplexity) – доступны следующие значения: 1 – включено, 0 – отключено;
   - «Время сброса счетчика попыток неудачного входа» (ResetLockoutCount) – указывается время в минутах, через которое количество неудачных попыток ввода пароля пользователя будет сброшено;
   - «Время блокировки после неудачных попыток» (LockoutDuration) – указывается длительность блокировки в минутах после превышения

количества неправильных попыток;
    - «Обратимое шифрование паролей» (ClearTextPassword) – доступны следующие значения: 0 – отключено, 1 – включено;
    - «Количество неправильных попыток ввода пароля до блокировки» (LockoutBadCount);
    - «Размер истории паролей» (PasswordHistorySize) – указывается количество предыдущих паролей, которые будут сохранены.
3) «Настройка аудита событий» (для всех настраиваемых значений доступны следующие значения: 0 – нет аудита; 1 – аудит успешных событий; 2 – аудит неудачных событий; 3 – аудит успешных и неудачных событий):
    - «Аудит системных событий» (AuditSystemEvents);
    - «Аудит отслеживания процессов» (AuditProcessTracking);
    - «Аудит использования привилегий» (AuditPrivilegeUse);
    - «Аудит изменений политик безопасности» (AuditPolicyChange);
    - «Аудит доступа к объектам» (AuditObjectAccess);
    - «Аудит входа в учетную запись» (AuditAccountLogon);
    - «Аудит доступа к объектам Active Directory» (AuditDSAccess);
    - «Аудит управления учетными записями» (AuditAccountManage);
    - «Аудит событий входа (успешный/неуспешный вход)» (AuditLogonEvents).
4) «Настройка привилегированных права» – нет настраиваемых значений.
5) «Настройка политик безопасности согласно шаблону» – нет настраиваемых значений.
6) «Настройка расширенных политик аудита» (для всех настраиваемых значений доступны следующие значения: 0 – нет аудита; 1 – аудит успешных событий; 2 – аудит неудачных событий; 3 – аудит

успешных и неудачных событий):

- «Изменение состояния безопасности»;
- «Расширение системы безопасности»;
- «Целостность системы»;
- «Драйвер IPSEC»;
- «Другие системные события»;
- «Вход в систему»;
- «Выход из системы»;
- «Блокировка учетной записи»;
- «Основной режим IPsec»;
- «Быстрый режим IPsec»;
- «Расширенный режим IPsec»;
- «Специальный вход»;
- «Другие события входа и выхода»;
- «Сервер сетевых политик»;
- «Заявки пользователей или устройств на доступ»;
- «Членство в группе»;
- «Файловая система»;
- «Реестр»;
- «Объект-задание»;
- «SAM»;
- «Службы сертификации»;
- «Создано приложением»;
- «Работа с дескриптором»;
- «Общий файловый ресурс»;
- «Отбрасывание пакета платформой фильтрации»;
- «Подключение платформы фильтрации»;
- «Другие события доступа к объекту»;
- «Сведения об общем файловом ресурсе»;
- «Съемные носители»;
- «Сверка с централизованной политикой»;
- «Использование прав, затрагивающих конфиденциальные данные»;
- «Использование прав, не затрагивающих конфиденциальные данные»;
- «Другие события использования прав»;
- «Создание процесса»;
- «Завершение процесса»;

- «Активность DPAPI»;
- «События RPC»;
- «Самонастраиваемые события»;
- «События изменений прав маркера»;
- «Аудит изменения политики»;
- «Изменение политики проверки подлинности»;
- «Изменение политики авторизации»;
- «Изменение политики правила уровня MPSSVC»;
- «Изменение политики платформы фильтрации»;
- «Другие события изменения политики»;
- «Управление учетными записями»;
- «Управление учетной записью компьютера»;
- «Управление группой безопасности»;
- «Управление группой распространения»;
- «Управление группой приложений»;
- «Другие события управления учетной записью»;
- «Доступ к службе каталогов»;
- «Изменения службы каталогов»;
- «Репликация службы каталогов»;
- «Подробная репликация службы каталогов»;
- «Проверка учетных данных»;
- «Операции с билетами службы Kerberos»;
- «Другие события входа учетных записей»;
- «Служба проверки подлинности Kerberos».

Примечания:

1) После применения настроек автоматически выполняется обновление групповых политик командой «gpupdate /force».
2) Для применения готового шаблона конфигурации используется утилита secedit.
3) Изменение некоторых параметров безопасности может потребовать перезагрузки системы для вступления в силу.

3.13.2. Примеры использования

3.13.2.1. Применение предустановленных настроек

Действия: Предустановленные настройки

Результат: на устройстве будут применены все настройки безопасности из предустановленного набора, включающего настройку параметров, представленных в таблице 16.

Таблица 16. Состав и описание параметров сценария

Политика	Описание	Значение
MaximumPasswordAge	Максимальный срок действия пароля	180 дней
MinimumPasswordAge	Минимальный срок действия пароля	1 день
MinimumPasswordLength	Минимальная длина пароля	10 символов
PasswordComplexity	Требование сложности пароля (использование букв разного регистра, цифр и спецсимволов)	1 (включено)
PasswordHistorySize	Количество запоминаемых паролей для предотвращения повторного использования	10 паролей
LockoutBadCount	Количество неудачных попыток ввода пароля до блокировки учетной записи	5 попыток
ResetLockoutCount	Время до сброса счетчика неудачных попыток входа	30 минут
LockoutDuration	Длительность блокировки учетной записи после превышения количества неудачных попыток	30 минут
ClearTextPassword	Хранение паролей в открытом виде	0 (отключено)
AuditSystemEvents	Аудит системных событий (загрузка/выключение, изменение системного времени и др.)	3 (успех и отказ)
AuditLogonEvents	Аудит событий входа в систему (локальный и сетевой вход)	3 (успех и отказ)
AuditAccountManage	Аудит управления учетными записями (создание, изменение, удаление учетных записей)	3 (успех и отказ)

AuditDSAccess	Аудит доступа к службе каталогов (изменения в Active Directory)	3 (успех и отказ)
AuditAccountLogon	Аудит проверки учетных данных при входе	3 (успех и отказ)
AuditObjectAccess	Аудит доступа к объектам (файлам, папкам, принтерам и др.)	3 (успех и отказ)
AuditPolicyChange	Аудит изменений политики безопасности	3 (успех и отказ)
AuditPrivilegeUse	Аудит использования привилегий пользователями	3 (успех и отказ)
AuditProcessTracking	Аудит запуска и завершения процессов	3 (успех и отказ)

Локальные групповые политики обновятся автоматически.

3.13.2.2. Настройка минимальной длины пароля

Действия: Настройка парольной политики
Настраиваемое значение: Минимальная длина пароля
Значение: 12

Результат: минимальная длина пароля для всех локальных учетных записей будет изменена на 12 символов. При следующей смене пароля пользователи должны будут использовать пароли длиной не менее 12 символов. Настройка вступает в силу после обновления групповых политик.

3.13.2.3. Включение аудита входа в систему

Действия: Настройка аудита событий
Настраиваемое значение: Аудит событий входа (успешный/неуспешный вход)
Значение: 3

Результат: в журнале событий Windows будут фиксироваться как успешные, так и неудачные попытки входа в систему (локальные и сетевые). Это позволит отслеживать активность пользователей и обнаруживать попытки несанкционированного доступа.

3.13.2.4. Настройка расширенного аудита создания процессов

Действия: Настройка расширенных политик аудита
Настраиваемое значение: Создание процесса
Значение: 1
Результат: система начнет записывать в журнал событий информацию о всех успешно запущенных процессах, включая имя исполняемого файла, путь, аргументы командной строки и пользователя, запустившего процесс. Создается CSV-файл конфигурации в папке групповых политик для применения настроек.

3.13.2.5. Применение шаблона политик безопасности

Действия: Настройка политик безопасности согласно шаблону
Файл шаблона политик безопасности: security_template.inf
Результат: все политики безопасности, указанные в файле шаблона, будут применены к системе через утилиту secedit.exe. Временный файл шаблона будет скопирован на устройство, применен и автоматически удален. Групповые политики обновятся принудительно командой «gpupdate /force».

Пример содержимого файла шаблона:

```inf
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 12
PasswordComplexity = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
[Privilege Rights]
SeNetworkLogonRight = *S-1-1-0,*S-1-5-32-544,*S-1-5-32-545
```

3.14. Переименование устройства

Код: SYS_HOSTNAME

Сценарий предназначен для автоматического переименования устройств по заданной политике именования. Система проверяет соответствие имен устройств настроенной политике именования. В случае несоответствия генерирует уникальные имена на основе префикса и числовой последовательности, ведет учет назначенных имен и предотвращает конфликты имен в сети.

3.14.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 17.

Таблица 17. Состав и описание параметров сценария

Название параметра	**Место заполнения**	**Описание**	**Обязательность**
Префикс	В задаче	Поле для указания префикса для генерации имени устройства, например: «WS-», «PC», «LAPTOP», «ARM»	Да
Начальное значение	В задаче	Поле для указания начального значения числового диапазона для генерации имен	Да
Конечное значение	В задаче	Поле для указания конечного значения числового диапазона для генерации имен	Да
Регулярное выражения для исключения	В задаче	Поле для указания регулярного выражения для исключения определенных имен из списка доступных для назначения. Примеры регулярных выражений: • ^.*TEST.*$ – исключить все имена, содержащие «TEST»; • ^WS(001|002|003)$ – исключить конкретные имена WS001, WS002, WS003; • ^.*[89]$ – исключить имена, заканчивающиеся на 8 или 9; • LAPTOP-10(1[3-6]|20) – исключить из назначения имена в диапазоне от LAPTOP-1013 до LAPTOP-1016, а также имя LAPTOP-1020	Да

Расположение файла	В задаче	Поле для указания пути расположения JSON-файла на сервере Ansible для ведения учета назначенных имен устройств. Пример: /tmp/CEDM_rename_history.json	Да
Действие перезагрузки	В задаче	Поле для выбора способа обработки перезагрузки устройства после переименования: • «Перезагрузить УРМ принудительно» – указать время, через которое устройство будет перезагружено автоматически. Пользователю оконечного устройства отобразится сообщение о перезагрузке через время, указанное в поле «Перезагрузить через»; • «Не перезагружать УРМ» – устройство не будет перезагружено. Изменения вступят в силу после перезагрузки устройства пользователем вручную	Да
Время до перезагрузки (в мин)	В задаче	Поле для указания времени в минутах, через которое устройство будет принудительно перезагружено. Если в поле «Действие перезагрузки» выбрано значение «Не перезагружать УРМ», то необходимо указать значение 0	Да

3.14.2. Примеры использования

3.14.2.1. Настройка политики именования для рабочих станций

Префикс: WS
Начальное значение: 1
Конечное значение: 100
Регулярное выражение для исключения: *^WS(090|091|092)$*
Расположение файла: /tmp/CEDM_rename_history.json
Действие перезагрузки: «Не перезагружать УРМ»
Перезагрузить через: 0

Результат: Система создаст политику именования, и осуществит переименование устройств, чьи имена не соответствуют политике. Будут присвоены имена от WS001 до WS100, за исключением WS090, WS091 и WS092. После переименования пользователям устройств будет показано уведомление о необходимости ручной перезагрузки. Информация о старых и новых именах устройств сохранится в файл учета для предотвращения конфликтов имен.

3.14.2.2. Настройка политики именования для ноутбуков с принудительной перезагрузкой

Префикс: LAPTOP
Начальное значение: 200
Конечное значение: 300
Регулярное выражение для исключения:
^LAPTOP(250|260|270)$
Расположение файла: /tmp/CEDM_rename_history.json
Действие перезагрузки: «Перезагрузить УРМ принудительно»
Перезагрузить через: 5
Результат: создается политика для ноутбуков с именами LAPTOP200-LAPTOP300, исключая LAPTOP250, LAPTOP260 и LAPTOP270. Если устройство уже имеет подходящее имя в этом диапазоне, переименование не выполняется. Новые устройства получают первое доступное имя. После успешного переименования система покажет уведомление пользователю о предстоящей перезагрузке и автоматически перезагрузит устройство через 5 минут.

3.15. Добавление устройства в домен

Код: SEC_AD

Сценарий предназначен для автоматического добавления оконечных устройств под управлением ОС Windows в домен Active Directory (AD). Сценарий автоматически находит свободное имя компьютера в заданном диапазоне, добавляет устройство в указанную организационную единицу (OU) домена и выполняет перезагрузку для применения изменений.

3.15.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 18.

Таблица 18. Состав и описание параметров сценария

Название параметра	**Место заполнения**	**Описание**	**Обязательность**
Основное действие	В шаблоне	Поле для выбора действия. Выбирается один из двух вариантов: • «Добавить устройство в домен AD» – устройство будет добавлено в домен Active Directory; • «Добавить устройство в рабочую группу» – устройство будет исключено из домена и добавлено в рабочую группу	Да
Способ формирования наименования устройства	В шаблоне	Поле для выбора способа формирования наименования устройства. Выбирается один из следующих вариантов: • «Свободное имя в OU» – устройство будет добавлено в домен Active Directory; • «Свободное имя из диапазона в OU – устройству будет присвоено первое свободное имя из указанного диапазона и OU; • «Текущее имя устройства» – имя устройства останется без изменений	Да
Протокол службы Active Directory	В шаблоне	Поле для выбора протокола подключения к Active Directory	Да
Домен	В шаблоне	Поле для указания DNS-имени домена AD, в который требуется добавить устройство	Да
Организационная единица (OU)	В шаблоне	Поле для указания пути к OU без полей DC. Например: OU=workstation,OU=Office1	Да

Время до перезагрузки (в мин)	В шаблоне	Поле для указания времени в минутах, через которое устройство будет перезагружено	Нет
Сохранять в журнале событий информацию о пропущенных действиях в шаблоне	В шаблоне	Поле для включения возможности сохранения в журнале событий информации о пропущенных действиях в шаблоне	Нет
Начальное значение диапазона	В шаблоне	Поле для указания начального значения диапазона для поиска свободного имени в OU и диапазоне	Нет
Конечное значение диапазона	В шаблоне	Поле для указания конечного значения диапазона для поиска свободного имени в OU и диапазоне	Нет
Префикс	В шаблоне	Поле для указания префикса для имени компьютера, к которому автоматически будет добавлен сгенерированный номер	Да
Имя пользователя	В задаче	Поле для указания имени пользователя технической учетной записи (ТУЗ) с правами добавления компьютеров в домен	Да
Пароль пользователя	В задаче	Поле для указания пароля от технической учетной записи	Да

3.15.2. Примеры использования

3.15.2.1. Добавление рабочей станции в корпоративный домен

Параметры шаблона:
Домен: corp.company.com
Уникальное имя домена: DC=corp
Минимальный номер АРМ: 001
Максимальный номер АРМ: 500
Количество символов в номере: 3
Префикс: WS-
Параметры задачи:
Имя пользователя: corp\pc-joiner
Пароль пользователя: [скрыт]

Результат: устройство будет добавлено в домен corp.company.com с именем WS-001 (или следующим доступным номером).

3.16. Управление WMI и WinRM

Код: SYS_WMI_WINRM

Сценарий предназначен для управления службами инструментария управления Windows (WMI) и служб удаленного управления Windows (WinRM) на оконечных устройствах. Позволяет настраивать права доступа к WMI-пространствам имен и управлять состоянием службы WinRM.

3.16.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 19.

Таблица 19. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Управление службами	В шаблоне	Поле для выбора службы для настройки. Доступны следующие варианты: • «Инструментарий управления Windows» – настройка прав доступа к пространствам имен WMI; • «Службы удаленного управления Windows (WinRM)» – управление состоянием и автозапуском службы WinRM	Да
Параметры	В шаблоне	Поле для выбора действий со службой. Указывается только при выборе в параметре «Управление службами» значения «Службы удаленного управления Windows (WinRM)». Доступны следующие варианты: • «Запуск и включение автозапуска службы WinRM» – запускает службу WinRM и настраивает автоматический запуск при загрузке системы; • «Остановка и отключение службы WinRM (Stop)» –	Нет

		останавливает службу WinRM и отключает автозапуск; • «Остановка службы без изменения настроек автозапуска» – останавливает службу WinRM, сохраняя текущие настройки автозапуска	
Имя пространства	В шаблоне	Поле для указания пространства имен WMI для настройки прав доступа. Указывается только при выборе в параметре «Управление службами» значения «Инструментарий управления Windows». Примеры пространств имен: • root\cimv2 – основное пространство имен для управления системой; • root\default – пространство имен по умолчанию; • root\wmi – пространство имен для драйверов и аппаратного обеспечения; • root\directory\ldap – пространство имен для работы с Active Directory	Нет
Аккаунт или Группа	В шаблоне	Поле для указания учетной записи или группы для настройки прав доступа. Указывается только при выборе в параметре «Управление службами» значения «Инструментарий управления Windows». Примеры: • DOMAIN\Username – доменная учетная запись; • Username – локальная учетная запись • BUILTIN\Administrators – встроенная группа администраторов; • user@domain.com – учетная запись в формате UPN	Нет
Действие	В шаблоне	Поле для выбора действий с правами доступа. Указывается только при выборе в параметре «Управление	Нет

		службами» значения «Инструментарий управления Windows». Доступны следующие варианты для выбора: • «Добавить» – добавить указанные права доступа для учетной записи или группы; • «Удалить» – удалить все права доступа для указанной учетной записи или группы	
Разрешения	В шаблоне	Поле для выбора прав доступа для назначения. Указывается только при выборе в параметре «Управление службами» значения «Инструментарий управления Windows». Доступны следующие варианты для выбора: • «PartialWrite» – частичная запись данных в пространство имен; • «Enable» – включает учетную запись и предоставляет пользователю права на чтение; • «ProviderWrite» – права записи через провайдеров WMI; • «ReadSecurity» – чтение настроек безопасности пространства имен; • «WriteSecurity» – изменение настроек безопасности пространства имен; • «MethodExecute» – разрешает выполнение методов. Провайдеры могут выполнять дополнительные проверки доступа. Это стандартное право доступа для всех пользователей; • «RemoteAccess» – удаленный доступ к пространству имен WMI	Нет

3.16.2. Режимы работы сценария

3.16.2.1. Управление службой WinRM

При выборе службы WinRM сценарий управляет состоянием службы Windows Remote Management:

- запуск службы: включает службу WinRM и настраивает автоматический запуск;
- остановка службы: полностью отключает службу WinRM и автозапуск;
- временная остановка: останавливает службу без изменения настроек автозапуска.

3.16.2.2. Управление правами доступа WMI

При выборе службы WMI сценарий настраивает права доступа к указанному пространству имен:
копирование PowerShell-скрипта на целевое устройство;
модификация дескриптора безопасности пространства имен WMI;
добавление или удаление ACE (Access Control Entry) для указанной учетной записи;
очистка временных файлов после выполнения операции.

3.16.3. Примеры использования

3.16.3.1. Включение службы WinRM для удаленного управления

Управление службами: «Службы удаленного управления Windows»

Параметры: запуск и включение автозапуска службы WinRM

Результат: служба WinRM будет запущена и настроена на автоматический запуск при загрузке системы. Это обеспечит возможность удаленного управления устройством через PowerShell Remoting, Windows Remote Shell (WinRS) и другие инструменты удаленного администрирования. Служба начнет принимать подключения на стандартных портах (HTTP: 5985, HTTPS: 5986).

3.16.3.2. Предоставление прав чтения WMI для службы мониторинга

Управление службами: «Инструментарий управления Windows»

Имя пространства: root\cimv2

Аккаунт или Группа: DOMAIN\MonitoringService

Действие: «Добавить»

Разрешения: «Enable»

Результат: Учетная запись DOMAIN\MonitoringService получит права на чтение данных из пространства имен root\cimv2, что

позволит службе мониторинга собирать информацию о системе, процессах, службах и другие данные через WMI. PowerShell-скрипт временно скопируется на устройство, выполнит настройку прав доступа и автоматически удалится.

3.16.3.3. Настройка прав выполнения методов WMI для администраторов

Управление службами: Инструментарий управления Windows

Имя пространства: root\default

Аккаунт или Группа: BUILTIN\Administrators

Действие: «Добавить»

Разрешения: MethodExecute

Результат: Группа администраторов получит права на выполнение методов WMI в пространстве имен root\default. Это позволит администраторам выполнять управляющие операции через WMI, такие как запуск процессов, управление службами и выполнение других административных задач. Права вступают в силу немедленно после применения.

3.16.3.4. Удаление прав доступа WMI для пользователя

Управление службами: Инструментарий управления Windows

Имя пространства: root\wmi

Аккаунт или Группа: DOMAIN\TestUser

Действие: «Удалить»

Результат: Все права доступа для учетной записи DOMAIN\TestUser будут удалены из пространства имен root\wmi. Пользователь больше не сможет получать доступ к аппаратным данным и информации драйверов через указанное пространство имен. Удаление выполняется полностью, убираются все существующие записи ACE для данной учетной записи.

3.16.3.5. Временная остановка службы WinRM для обслуживания

Управление службами: «Службы удаленного управления Windows»

Параметры: «Остановка службы без изменения настроек автозапуска»

Результат: служба WinRM будет остановлена, но настройки автозапуска останутся неизменными. Это полезно для временного прекращения удаленных подключений во время обслуживания системы или установки обновлений. После перезагрузки система автоматически запустит службу, если она была настроена на автозапуск.

3.16.3.6. Предоставление удаленного доступа к WMI для группы операторов

Управление службами: «Инструментарий управления Windows»

Имя пространства: root\cimv2

Аккаунт или Группа: DOMAIN\Operators

Действие: «Добавить»

Разрешения: «RemoteAccess»

Результат: группа DOMAIN\Operators получит права удаленного доступа к пространству имен root\cimv2 через WMI. Члены группы смогут подключаться к WMI на данном устройстве удаленно с других компьютеров в сети для мониторинга и управления системными ресурсами. Доступ будет предоставлен в соответствии с дополнительными настройками DCOM и брандмауэра Windows.

3.17. Удаление программного обеспечения

Код: SFT_UNINST

Сценарий предназначен для централизованного удаления программного обеспечения с оконечных устройств с ОС Windows. Использует данные инвентаризации для автоматического определения установленного ПО и выполняет интеллектуальное удаление через GUID или строку деинсталляции.

3.17.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 20.

Таблица 20. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Значение фильтра	В шаблоне	Поле для выбора фильтра из списка, который содержит названия и версии	Да

		программного обеспечения, собранные со всех зарегистрированных оконечных устройств в ходе инвентаризации	
Действие при дубле	В шаблоне	Поле для выбора действий в случае дублирования УРМ в рамках сценария: • «Выполнить первый»; • «Пропустить УРМ»	Да

Примечание: если выбранное программное обеспечение отсутствует на устройстве, то задача на таком устройстве выполняться не будет.

3.18. Управление сетевыми настройками

Код: SYS_NETWORK

Сценарий предназначен для централизованного управления сетевыми подключениями на оконечных устройствах. Позволяет добавлять профили подключения как из готовых XML-файлов, так и путем создания новых профилей, а также управлять сетевыми адаптерами и удалять существующие профили.

3.18.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 21.

Таблица 21. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Файл Wi-Fi профиль	В шаблоне	Поле для выбора XML-файла с готовым профилем Wi-Fi подключения для импорта в систему	Нет
Тип сетевого оборудования	В шаблоне	Поле для выбора типа сетевого оборудования для управления. Выбирается один из двух вариантов: • «Wi-Fi» – управление беспроводными сетевыми подключениями; • «Ethernet» – управление проводными сетевыми адаптерами	Да
Действие	В шаблоне	Поле для выбора действий, которые будут выполнены с сетевым оборудованием. Доступные значения при выборе Wi-Fi:	Да

		• «Импорт Wi-Fi профиля» – установка готового профиля из XML-файла, указанного в поле «Файл Wi-Fi профиля»; • «Создание и установка нового профиля WPA/WPA2» – создание нового профиля с защитой WPA/WPA2 с использованием данных, указанных в полях «Имя профиля/адаптера», «SSID». Пароль задается в задаче; • «Удаление существующего профиля» – удаление профиля Wi-Fi, указанного в поле «Имя профиля/адаптера». Доступные значения при выборе Ethernet: • «Список установленных Ethernet-адаптеров» – отображение информации о всех сетевых адаптерах системы; • «Включить сетевой адаптер» – активация сетевого адаптера, указанного в поле «Имя профиля/адаптера»; • «Выключить сетевой адаптер» – деактивация сетевого адаптера, указанного в поле «Имя профиля/адаптера»	
Имя профиля/адаптера	В шаблоне	Поле для указания имени профиля Wi-Fi или имени сетевого адаптера в зависимости от выбранного действия	Нет
SSID	В шаблоне	Поле для указания SSID (имя) беспроводной сети для создания нового профиля Wi-Fi	Нет
Пароль	В задаче	Поле для указания пароля создаваемого Wi-Fi профиля (отображается скрытым при вводе)	Нет

3.18.2. Структура XML-профиля Wi-Fi

Ниже приведена структура XML-профиля Wi-Fi для использования в сценарии

```xml
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
  <name>Имя_профиля</name>
  <SSIDConfig>
    <SSID>
      <hex>HEX_представление_SSID</hex>
      <name>SSID_сети</name>
    </SSID>
  </SSIDConfig>
  <connectionType>ESS</connectionType>
  <connectionMode>auto</connectionMode>
  <MSM>
    <security>
      <authEncryption>
        <authentication>WPA2PSK</authentication>
        <encryption>AES</encryption>
        <useOneX>false</useOneX>
      </authEncryption>
      <sharedKey>
        <keyType>passPhrase</keyType>
        <protected>false</protected>
        <keyMaterial>пароль</keyMaterial>
      </sharedKey>
    </security>
  </MSM>
</WLANProfile>
```

3.18.3. Примеры использования

3.18.3.1. Создание и тиражирование корпоративного Wi-Fi профиля

Тип сетевого оборудования: Wi-Fi
Действие: «Создание и установка нового профиля WPA/WPA2»
Имя профиля/адаптера: Corporate_Network
SSID: COMPANY_WIFI
Пароль: SecurePassword123

Результат: на устройствах будет создан и установлен новый Wi-Fi профиль с именем «Corporate_Network» для подключения к корпоративной сети «COMPANY_WIFI». Система автоматически сгенерирует HEX-представление SSID, создаст XML-конфигурацию с защитой WPA2PSK/AES и установит профиль через netsh. Временные файлы будут автоматически удалены. Пользователи смогут подключаться к сети автоматически при ее обнаружении.

3.18.3.2. Тиражирование готового Wi-Fi профиля

Файл Wi-Fi профиль: guest_network.xml
Тип сетевого оборудования: Wi-Fi
Действие: «Импорт Wi-Fi профиля»
Результат: готовый XML-профиль будет загружен на устройства и установлен в систему. Файл временно копируется в папку кеша, устанавливается через команду «netsh wlan add profile», после чего временный файл удаляется. Профиль станет доступен для подключения сразу после установки с сохранением всех настроек из исходного XML-файла.

3.18.3.3. Удаление устаревшего Wi-Fi профиля

Тип сетевого оборудования: Wi-Fi
Действие: «Удаление существующего профиля»
Имя профиля/адаптера: Old_Guest_Network
Результат: профиль «Old_Guest_Network» будет полностью удален из системы с помощью команды «netsh wlan delete profile». Устройство больше не сможет автоматически подключаться к этой сети, и профиль исчезнет из списка доступных подключений в настройках Wi-Fi.

3.18.3.4. Получение информации о сетевых адаптерах

Тип сетевого оборудования: Ethernet
Действие: «Список установленных Ethernet-адаптеров»
Результат: система в выводе Ansible отобразит полную информацию о всех сетевых адаптерах устройств, включая их имена, текущий статус (включен/отключен) и описание интерфейса. Информация будет показана в журнале событий выполнения сценария для анализа администратором.

3.18.3.5. Отключение запрещенного к использованию сетевого интерфейса

Тип сетевого оборудования: Ethernet
Действие: «Выключить сетевой адаптер»
Имя профиля/адаптера: Ethernet 2
Результат: сетевой интерфейс «Ethernet 2» будет деактивирован с помощью команды «Disable-NetAdapter» в PowerShell без запроса подтверждения пользователя. Сетевое подключение через этот адаптер будет прервано, но драйвер останется установленным. Адаптер можно будет активировать позже с помощью соответствующей команды или интерфейса системы.

3.19. Управление службами

Код: SYS_SERVICES

Сценарий предназначен для централизованного управления системными службами ОС Windows на оконечных устройствах. Позволяет запускать, останавливать, перезапускать службы, а также настраивать режимы их автоматического запуска.

3.19.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 22.

Таблица 22. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Управление состоянием службы	В шаблоне	Поле для выбора действий для управления текущим состоянием службы. Доступны следующие значения: • «Запуск службы (start)» – запускает остановленную службу; • «Остановка службы (stop)» – останавливает работающую службу; • «Перезапуск службы (restart)» – перезапускает службу	Да
Настройка режима	В шаблоне	Поле для выбора режима автоматического запуска службы при	Нет

запуска службы		загрузке системы. Доступны следующие значения: • «Автоматический запуск службы» при старте системы (auto) – служба запускается автоматически при загрузке ОС; • «Автоматический запуск службы с задержкой (delayed)» – служба запускается автоматически, но с задержкой после загрузки системы для ускорения старта ОС; • «Ручной запуск службы (manual)» – служба запускается только по требованию пользователя или другой службы; • «Отключение службы (disabled) – служба останавливается и блокируется возможность ее запуска	
Имя службы	В шаблоне	Поле для указания системного имени службы	Да

3.19.2. Примеры использования

3.19.2.1. Запуск службы Windows Update с автоматическим режимом

Управление состоянием службы: «Запуск службы»

Настройка режима запуска службы: «Автоматический запуск службы при старте системы»

Имя службы: wuauserv

Результат: служба Центра обновления Windows будет немедленно запущена и настроена на автоматический запуск при каждой загрузке ОС. Это обеспечит регулярное получение и установку обновлений безопасности. Изменения вступают в силу мгновенно, и служба начнет проверку доступных обновлений в соответствии с настроенным расписанием.

3.19.2.2. Остановка службы диспетчера печати для обслуживания

Управление состоянием службы: «Остановка службы»

Настройка режима запуска службы: «Ручной запуск службы»

Имя службы: spooler

Результат: служба диспетчера печати будет остановлена, что прекратит все задания печати и освободит очередь принтера. Режим запуска изменится на ручной, что предотвратит автоматический запуск службы при перезагрузке.

3.19.2.3. Перезапуск службы времени для синхронизации

Управление состоянием службы: Перезапуск службы»

Имя службы: w32time

Результат: служба времени Windows будет перезапущена, что принудительно запустит процесс синхронизации времени с настроенным NTP-сервером. Это поможет устранить проблемы с неточным временем на устройстве. Перезапуск выполняется корректно с сохранением всех настроек службы и не влияет на режим автозапуска.

3.19.2.4. Отключение ненужной службы для повышения безопасности

Управление состоянием службы: «Остановка службы»

Настройка режима запуска службы: «Отключение службы»

Имя службы: telnet

Результат: служба Telnet будет остановлена и полностью отключена, что заблокирует возможность ее запуска. Это повышает безопасность системы, удаляя потенциальную точку входа для злоумышленников. Служба не будет запускаться автоматически при загрузке системы или по требованию других приложений до изменения режима запуска обратно на разрешенный.

3.19.2.5. Настройка службы BITS с отложенным запуском

Управление состоянием службы: «Запуск службы»

Настройка режима запуска службы: «Автоматический запуск службы с задержкой»

Имя службы: bits

Результат: фоновая интеллектуальная служба передачи будет запущена и настроена на автоматический запуск с задержкой при загрузке системы. Это ускорит процесс загрузки Windows, т. к. служба запустится после завершения инициализации критически важных компонентов. Служба обеспечит фоновую загрузку

обновлений и других файлов без влияния на производительность системы.

3.19.2.6. Запуск службы журнала событий в ручном режиме

Управление состоянием службы: «Запуск службы»

Настройка режима запуска службы: «Ручной запуск службы»

Имя службы: eventlog

Результат: служба журнала событий Windows будет запущена немедленно, но настроена на ручной режим запуска. Это означает, что служба будет работать в текущем сеансе, но после перезагрузки ОС потребует ручного запуска или запуска по требованию другой службы. Журналирование событий возобновится, что важно для диагностики и мониторинга системы.

3.20. Управление реестром

Код: SYS_REGISTRY

Сценарий предназначен для централизованного управления реестром ОС Windows на оконечных устройствах. Позволяет импортировать готовые REG-файлы реестра, а также выполнять операции создания, изменения и удаления разделов и параметров реестра.

3.20.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 23.

Таблица 23. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Файл реестра	В шаблоне	Поле для выбора REG-файла реестра для импорта в систему	Нет
Действие	В шаблоне	Поле для выбора действий с реестром. Доступные следующие значения: • «Импортировать файл реестра» – импорт готового REG- файла в реестр системы; • «Создать раздел реестра» – создает указанный раздел реестра, включая все промежуточные разделы в пути;	Да

		• «Добавление параметра реестра» – создает параметр реестра с указанным именем, значением и типом данных в заданном разделе; • «Обновление значения параметра реестра» – обновляет параметр реестра с указанным именем, значением и типом данных в заданном разделе; • «Удаление раздела реестра» – удаляет указанный раздел реестра и все его содержимое; • «Удаление параметра реестра» – удаляет указанный параметр реестра из заданного раздела	
Путь раздела реестра	В шаблоне	Поле для указания укажите полного пути в реестре. Например: HKLM:\SOFTWARE\CEDM\TEST	Нет
Имя в реестре	В шаблоне	Поле для указания имени параметра реестра для создания, изменения или удаления	Нет
Значение	В шаблоне	Поле для указания значения для параметра реестра	Нет
Тип	В шаблоне	Поле для выбора типа данных для параметра реестра. Доступны следующие значения: • «Неопределенный тип» – используется, когда значение записи не имеет конкретного типа или оно неопределенно; • «Двоичные данные» – используется для хранения произвольных двоичных данных, например, значений, которые не могут быть представлены в виде строки; • «32-битное целое число» – 32-битное целое число. Часто используется для хранения числовых параметров конфигурации;	Нет

		• «64-битное целое число» – 64-битное целое число. Используется для хранения более крупных чисел, чем DWORD; • «Строка» – строковый тип данных. Используется для хранения текстовых значений, например, путей, имен и прочих текстовых данных; • «Строка с возможностью расширения» – строка, содержащая переменные окружения, такие как %SystemRoot%, которые могут быть автоматически расширены системой при их использовании; • «Множественные строки» – список строк, разделенных символом нулевой длины. Используется, когда необходимо хранить несколько значений, например, пути к папкам или элементам	

3.20.1. Примеры использования

3.20.1.1. Импорт корпоративных настроек из файла реестра

Файл реестра: corporate_settings.reg
Действие: «Импортировать файл реестра»
Результат: готовый файл реестра «corporate_settings.reg» будет скопирован на устройство и импортирован в системный реестр с помощью команды «reg import». Все настройки из файла будут применены немедленно, включая параметры групповых политик, настройки приложений и системные конфигурации. Временный файл будет автоматически удален после импорта для обеспечения безопасности.

3.20.1.2. Создание раздела для настроек приложения

Действие: «Создать раздел реестра»
Путь раздела реестра: *HKLM\SOFTWARE\MyCompany\MyApplication*
Результат: в реестре будет создан новый раздел по указанному пути, включая все промежуточные разделы, если они не

существуют. Это подготовит структуру реестра для размещения настроек пользовательского приложения. Раздел будет доступен для всех пользователей системы, поскольку создается в ветке HKEY_LOCAL_MACHINE.

3.20.1.3. Добавление параметра автозапуска приложения

Действие: «Добавление параметра реестра»
Путь раздела реестра:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Имя в реестре: MyApplication
Значение: *C:\Program Files\MyCompany\MyApp.exe*
Тип: Строка
Результат: в разделе автозапуска текущего пользователя будет создан новый параметр «MyApplication» со строковым значением, содержащим путь к исполняемому файлу. Это обеспечит автоматический запуск приложения при входе пользователя в систему. Параметр будет активен для текущего пользователя и не повлияет на других пользователей компьютера.

3.20.1.4. Настройка числового параметра конфигурации

Действие: «Обновление значения параметра реестра»
Путь раздела реестра: *HKLM:\SOFTWARE\MyCompany\Settings*
Имя в реестре: MaxConnections
Значение: 100
Тип: 32-битное целое число
Результат: параметр «MaxConnections» в указанном разделе будет обновлен или создан (если не существует) со значением 100 и типом DWORD. Это позволит приложению считывать числовое значение конфигурации из реестра. Изменение применится немедленно и будет доступно всем процессам, обращающимся к этому параметру.

3.20.1.5. Удаление требуемого параметра реестра

Действия: «Удаление параметра реестра»
Путь раздела реестра:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Имя в реестре: OldApplication
Результат: параметр «OldApplication» будет удален из раздела автозапуска, что предотвратит автоматический запуск устаревшего

приложения при входе пользователя в систему. Сам раздел «Run» останется нетронутым вместе с другими параметрами автозапуска. Изменение вступит в силу при следующем входе пользователя в систему.

3.20.1.6. Удаление раздела с настройками удаленного приложения

Действия: Удаление раздела реестра
Путь раздела реестра: *HKLM\SOFTWARE\RemovedApplication*
Результат: весь раздел «RemovedApplication» будет полностью удален из реестра вместе со всеми подразделами и параметрами. Это очистит систему от остатков конфигурации удаленного приложения, освободив место в реестре и устранив потенциальные конфликты. Операция необратима, поэтому следует убедиться в правильности указанного пути.

3.20.1.7. Создание переменной окружения через реестр

Действия: Добавление параметра реестра
Путь раздела реестра:
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment
Имя в реестре: COMPANY_HOME
Значение: %ProgramFiles%\MyCompany
Тип: Строка с возможностью расширения
Результат: будет создана системная переменная окружения «COMPANY_HOME» со значением, которое автоматически расширится до полного пути (например, *C:\Program Files\MyCompany*). Переменная будет доступна всем пользователям и процессам в системе после перезагрузки или обновления переменных окружения. Это позволит приложениям использовать стандартизированные пути к корпоративным ресурсам.

3.21. Управление правами доступа к файловой системе

Код: SEC_MGMT_ACL

Сценарий предназначен для централизованного управления списками управления доступом (ACL – Access Control List) к файлам и каталогам на оконечных устройствах под управлением ОС Windows. ACL определяет, какие пользователи или группы получают доступ к файлам и каталогам, а также какие операции они могут с ними

выполнять. Сценарий позволяет массово настраивать разрешения для пользователей и групп на основе CSV-файла с параметрами.

3.21.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 24.

Таблица 24. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
CSV-файл со списками ACL	В шаблоне	Поле для выбора CSV-файла с настройками прав доступа для применения к файлам и каталогам	Да

Списки ACL загружаются в Систему в виде CSV-файла, где столбцы разделены точкой с запятой. Файл должен содержать следующие обязательные колонки:

- type – тип операции:
  - add – добавить права доступа;
  - remove – удалить права доступа;
- path – полный путь к файлу или каталогу;
- group_users – имя пользователя или группы;
- rights – устанавливаемые права доступа. Возможные значения: FullControl, Modify, ReadAndExecute, Read, Write, Delete;
- inherit – тип наследования прав:
  - allow – разрешающие права доступа;
  - deny – запрещающие права доступа;
- Inheritance – флаги наследования:
  - ContainerInherit – наследование для контейнеров (папок);
  - ObjectInherit – наследование для объектов (файлов);
  - ContainerInherit,ObjectInherit – комбинация флагов;
- Propagation – флаги распространения прав:
  - None – обычное распространение;
  - InheritOnly – только наследование;
  - NoPropagateInherit – не распространять

наследование.

3.21.2. Примеры использования

3.21.2.1. Настройка прав доступа для корпоративной файловой структуры

Содержимое CSV-файла:

```
XML
type;path;group_users;rights;inherit;Inheritance;Propagation
add;C:\CorporateData;DOMAIN\AllUsers;ReadAndExecute;allow;ContainerInherit,ObjectInherit;None
add;C:\CorporateData\HR;DOMAIN\HR_Team;FullControl;allow;ContainerInherit,ObjectInherit;None
add;C:\CorporateData\Finance;DOMAIN\Finance_Team;Modify;allow;ContainerInherit,ObjectInherit;None
remove;C:\CorporateData;Everyone;Write;allow;ContainerInherit,ObjectInherit;None
```

Результат: система применит комплексную настройку прав доступа к корпоративной файловой структуре. Папка «C:\CorporateData» получит права чтения и выполнения для всех пользователей домена, специализированные подпапки HR и Finance получат расширенные права для соответствующих команд, а возможность записи для группы «Everyone» будет удалена для повышения безопасности. Все изменения применятся рекурсивно ко всем вложенным файлам и папкам.

3.21.2.2. Ограничение доступа к системным каталогам

CSV-файл содержимое:

```
XML
type;path;group_users;rights;inherit;Inheritance;Propagation
remove;C:\Windows\System32;Users;Write;allow;ContainerInherit,ObjectInherit;None
remove;C:\Windows\System32;Users;Delete;allow;ContainerInherit,ObjectInherit;None
add;C:\Windows\System32;Administrators;FullControl;allow;ContainerInherit,ObjectInherit;None
```

Результат: из системной папки System32 будут удалены права записи и удаления для обычных пользователей, что повысит

безопасность системы и предотвратит случайное повреждение критически важных системных файлов. Права полного контроля останутся только у администраторов. Эти изменения помогут защитить систему от несанкционированных изменений и вредоносного ПО.

3.21.2.3. Создание безопасной папки обмена файлами

CSV-файл содержимое:

```
XML
type;path;group_users;rights;inherit;Inheritance;Propagation
add;C:\FileExchange;DOMAIN\AllUsers;Write;allow;ObjectInherit;None
add;C:\FileExchange;DOMAIN\AllUsers;ReadAndExecute;allow;ContainerInherit;None
remove;C:\FileExchange;DOMAIN\AllUsers;Delete;allow;ContainerInherit,ObjectInherit;None
add;C:\FileExchange;Administrators;FullControl;allow;ContainerInherit,ObjectInherit;None
```

3.22. Управление службой обновлений Windows

Код: SYS_WU

Сценарий предназначен для централизованной настройки параметров службы обновлений на оконечных устройствах под управлением ОС Windows. Позволяет управлять режимом работы службы Windows Update, расписанием установки обновлений и другими параметрами автоматического обновления.

3.22.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 25.

Таблица 25. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Настройки	В шаблоне	Поле для управление режимом работы службы ОС для обновления. Доступны следующие настройки: • «Применение предустановленной конфигурации» – будут применены настройки согласно политике безопасности;	Да

		• «Автоматическое обновление» – включение и отключение автоматического обновления (0 – включение, 1 – отключение); • «Режим автоматического обновления» – управление режимом автоматического обновления (2 – уведомлять перед загрузкой, 3 – загружать и уведомлять об установке, 4 – загрузка и установка по расписанию, 5 – разрешить пользователям настраивать параметры; • «Установка дня недели для обновлений» – указание дня недели, в который будет проводится обновление (0 – ежедневно, 1 – воскресенье, 2 – понедельник, 3 – вторник, 4 – среда, 5 – четверг, 6 – пятница, 7 – суббота); • «Установка времени для обновлений» – указание времени, в которое будет проводится обновление (0-23 – час установки обновлений, 24 – автоматическая установка времени)	
Устанавливаемое значение	В шаблоне	Поле для указания значений настроек. Устанавливаемое значение зависит от выбора типа настройки	Нет

3.22.2. Примеры использования

3.22.2.1. Применение стандартной корпоративной конфигурации

Настройки: «Применение предустановленной конфигурации»

Результат: на устройстве будет применена оптимальная корпоративная конфигурация Windows Update:
включены автоматические обновления;
активирована установка во время автоматического обслуживания;
настроена автоматическая загрузка обновлений с уведомлением

пользователя перед установкой;
установка планируется ежедневно в автоматически выбираемое системой время;
служба Windows Update будет запущена и настроена на автоматический старт.

3.23. Установка обновлений

Код: SEC_WU

Сценарий предназначен для централизованной установки обновлений ОС Windows на оконечных устройствах. Позволяет устанавливать все доступные обновления, обновления определенных категорий или конкретные обновления по номерам KB (Knowledge Base) с автоматической перезагрузкой при необходимости.

3.23.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 26.

Таблица 26. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Действие	В шаблоне	Поле для выбора типа устанавливаемых обновлений. Доступны следующие значения: • «Установить все обновления» – устанавливает все доступные обновления ОС Windows независимо от категории; • «Установить конкретную категорию обновлений» – устанавливает обновления только выбранной категории; • «Установить необходимый(-ые) KB» – устанавливает конкретные обновления по их номерам KB	Да
Категория обновлений	В шаблоне	Поле для выбора категории обновлений для установки. Поле доступно для заполнения только при выборе действия «Установить конкретную категорию обновлений». Доступные следующие значения:	Нет

		• «Критические обновления» – критически важные исправления для обеспечения стабильности и безопасности системы; • «Обновления безопасности» – исправления уязвимостей безопасности и защитные обновления; • «Сводные обновления» – комплексные пакеты обновлений, включающие несколько исправлений; • «Сервисные пакеты» – крупные наборы обновлений и новых функций; • «Обновления определений» – обновления антивирусных баз и определений безопасности; • «Наборы разработчика» – инструменты и компоненты для разработчиков; • «Функциональные обновления» – дополнительные функции и возможности системы	
Перечень устанавливаемых KB	В шаблоне	Поле для указания номеров KB для установки конкретных обновлений. Если необходимо указать более одного значения, то в качестве разделителя требуется использовать точку с запятой	Нет

3.23.2. Примеры использования

Действие: «Установить конкретную категорию обновлений»
Категория обновлений: Обновления безопасности
Результат: будут установлены только обновления категории «SecurityUpdates», которые устраняют уязвимости безопасности и повышают защищенность системы. Это обеспечивает быстрое закрытие критических брешей в безопасности без установки функциональных обновлений, которые могут повлиять на стабильность производственных систем. Устройство перезагрузится автоматически при необходимости.

3.23.2.1. Установка конкретных обновлений по номерам KB

Действие: «Установить необходимый(-ые) KB»

Перечень устанавливаемых KB: *KB5034439;KB5034441;KB5034442*

Результат: будут установлены только три указанных обновления: KB5034439, KB5034441 и KB5034442. Система найдет эти обновления во всех доступных категориях и установит их последовательно. Это позволяет точно контролировать, какие именно исправления применяются к системе, что критически важно для тестирования совместимости или соответствия корпоративным политикам обновлений.

3.24. Управления параметрами журналов событий Windows

Код: SYS_WEVT

Сценарий предназначен для централизованной настройки параметров системных журналов событий Windows (Event Log) на оконечных устройствах. Позволяет управлять настройками журналов безопасности, системных событий и событий приложений.

3.24.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 27.

Таблица 27. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Тип журнала событий	В шаблоне	Поле для выбора типа журнала событий для настройки. Доступны следующие значения: • «Журнал безопасности (Security)» – настройка параметров журнала событий безопасности Windows; • «Системный журнал (System)» – настройка параметров системного журнала событий Windows; • «Журнал приложений (Application)» – настройка параметров журнала событий приложений Windows	Да
Параметр журнала событий	В шаблоне	Поле для выбора параметра журнала событий для изменения. Доступны следующие значения:	Да

		• «Автоматическое резервное копирование файлов журнала» – включение/отключение автоматического создания резервных копий файлов журнала при достижении максимального размера; • «Максимальный размер журнала» – установка максимального размера файла журнала в байтах (по умолчанию 20971520 байт = 20 Мб); • «Верхний предел размера журнала» – установка верхнего предела размера журнала для дополнительного контроля; • «Ограничение доступа для гостевых учетных записей (RestrictGuestAccess)» – запрет доступа к журналу событий для гостевых учетных записей (повышение безопасности); • «Политика хранения событий (Retention)» – настройка политики сохранения событий при заполнении журнала	
Значение	В шаблоне	Поле для указания нового значения для выбранного параметра журнала	Да

3.24.2. Примеры использования

3.24.2.1. Увеличение размера журнала безопасности

Тип журнала событий: «Журнал безопасности»

Параметр журнала событий: «Максимальный размер журнала»

Значение: 104857600

Результат: максимальный размер журнала безопасности будет увеличен до 100 Мб (104857600 байт). Это позволит хранить больше событий безопасности до перезаписи старых записей. Изменение применяется немедленно и начинает действовать при следующей записи событий.

3.24.2.2. Включение резервного копирования системного журнала

Тип журнала событий: «Системный журнал»

Параметр журнала событий: «Автоматическое резервное копирование файлов журнала»

Значение: 1

Результат: при достижении максимального размера системного журнала Windows автоматически создаст резервную копию текущего файла журнала перед его очисткой. Резервные копии сохраняются в той же папке с уникальными именами, что обеспечивает сохранность исторических данных.

3.24.2.3. Ограничение доступа гостей к журналу приложений

Тип журнала событий: «Журнал приложений»

Параметр журнала событий: «Ограничение доступа для гостевых учетных записей»

Значение: 1

Результат: гостевые учетные записи больше не смогут читать события из журнала приложений, что повышает безопасность системы. Доступ к журналу будут иметь только пользователи с соответствующими привилегиями. Изменение вступает в силу немедленно.

3.24.2.4. Настройка политики хранения журнала безопасности

Тип журнала событий: «Журнал безопасности»

Параметр журнала событий: «Политика хранения событий»

Значение: 604800

Результат: события в журнале безопасности будут сохраняться в течение 7 дней (604800 секунд) перед возможной перезаписью. Это обеспечивает достаточное время для анализа событий безопасности и соответствует многим корпоративным политикам аудита.

3.24.2.5. Установка верхнего предела размера системного журнала

Тип журнала событий: «Системный журнал»

Параметр журнала событий: «Верхний предел размера журнала»

Значение: 209715200

Результат: устанавливается дополнительное ограничение в 200 Мб для системного журнала, что предотвращает неконтролируемое разрастание файла журнала и обеспечивает дополнительный контроль над использованием дискового пространства.

3.25. Сброс операционной системы

Код: SEC_WIPE

Сценарий предназначен для централизованного восстановления первоначальных настроек операционный системы Windows на оконечных устройствах и удаления профилей пользователей. Используется для подготовки устройств к передаче, решения проблем с поврежденными профилями или обеспечения безопасности данных.

Важно: данный сценарий выполняет необратимые операции, которые могут привести к полной потере данных.

3.25.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 28.

Таблица 28. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Действия	В шаблоне	Поле для выбора типа действия. Доступны выбор одного из двух вариантов: • «Удаление профиля пользователя» – удаление УЗ пользователя и всех связанных с ней данных; • «Сброс устройства к заводским настройкам» – запуск процесса полного сброса устройства с удалением всех пользовательских данных и настроек	Да
Имя профиля	В шаблоне	Поле для указания имени профиля, который будет удален. Указывается, если выбран тип действия «Удаление профиля пользователя»	Нет

3.25.2. Примеры использования

3.25.2.1. Удаление профиля пользователя

Действия: «Удаление профиля пользователя»
Имя профиля: ivanov.a
Результат выполнения сценария: сеанс пользователя «ivanov.a» будет завершен, а профиль и все пользовательские данный полностью удалены.

В результате удаления профиля пользователя очищаются следующие элементы:

- пользовательские файлы и папки, хранящиеся в директории профиля (обычно C:\Users\[Имя пользователя]);
- персональные настройки пользователя, включая настройки рабочего стола, меню «Пуск», и другие пользовательские конфигурации;
- установленные пользователем приложения, если они были установлены только для этого пользователя;
- данные приложений, хранящиеся в профиле пользователя;
- кеш и временные файлы, связанные с профилем;
- ключи реестра, относящиеся к данному профилю пользователя.

Удаление профиля не затрагивает:

- общесистемные настройки;
- приложения, установленные для всех пользователей;
- профили других пользователей;
- данные, хранящиеся вне профиля пользователя, например, на других разделах жесткого диска.

3.25.2.2. Сброс устройства к заводским настройкам

Действия: «Сброс устройства к заводским настройкам»
Имя профиля: (не требуется)
Результат выполнения сценария: устройство возвращено к первоначальному состоянию.

Выполнен полный сброс устройств с удалением всех пользовательских данных и настроек. Сценарий может быть использован в следующих случаях:

- при смене пользователя устройства;
- при передаче устройства другому сотруднику;
- при увольнении сотрудника;
- при утере или хищении устройства;
- при возникновении проблем с устройством.

Важно отметить, что хотя удаление профиля является необратимым процессом, оно менее радикально, чем полный сброс устройства. Удаление профиля затрагивает только данные и настройки конкретного пользователя, в то время как сброс устройства очищает всю систему.

3.26. Управление Kaspersky Endpoint Security

Код: SFT_MGMT_KES

Сценарий предназначен для выполнения настраиваемых команд управления и запуска готовых профилей, предоставляемых Kaspersky Endpoint Security.

3.26.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 29.

Таблица 29. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Основные действие	В шаблоне	Поле для выбора основного действия. Доступны следующие значения для выбора: • «Поиск вредоносного ПО» – запуск проверки системы на наличие вирусов, троянских программ и другого вредоносного ПО; • «Обновление баз и модулей приложения» – скачивание и установка последних антивирусных баз и компонентов Kaspersky Endpoint Security; • «Откат последнего обновления» – отмена последнего обновления баз или модулей и возврат к предыдущей версии;	Да

		• «Запуск профиля» – запуск выполнения профиля. Например, обновление баз или активация компонентов защиты; • «Остановка профиля» – остановка выполняемого профиля (требуется наличие прав администратора Kaspersky Endpoint Security); • «Запуск программы» – запуск Kaspersky Endpoint Security; • «Завершение работы программы» – завершение работы Kaspersky Endpoint Security с полной выгрузкой из оперативной памяти компьютера	
Отображение пропущенных задач	В задаче	Необходимость отображения пропущенных задач. Выбирается один из двух вариантов: • «Да» – пропущенные задачи будут отображены; • «Нет» – пропущенные задачи не будут отображены. Данное значение является значением по умолчанию	Нет
Имя пользователя	В задаче	Имя учетной записи пользователя, являющегося администратором Kaspersky Endpoint Security	Нет
Пароль	В задаче	Пароль учетной записи пользователя, являющегося администратором Kaspersky Endpoint Security. При вводе будет скрыт звездочками	Нет
Файл с параметрами	В шаблоне. Только для типа действий «Поиск вредоносного ПО» и «Обновление баз и модулей	Поле для выбора файла с параметрами. Поддерживаются файлы формата TXT.	Нет

	приложения»		
Действие при обнаружении угрозы	В шаблоне. Только для типа действия «Поиск вредоносного ПО»	Поле для выбора действий при обнаружении угрозы. Доступны следующие значения для выбора: • «Информировать» – при обнаружении зараженных файлов Kaspersky Endpoint Security только записывает информацию о них в список активных угроз без каких-либо действий над файлами; • «Лечить. Информировать, если лечение невозможно» – приложение автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то информация об обнаруженных зараженных файлах будет добавлена в список активных угроз; • «Лечить. Удалять, если лечение невозможно» – приложение автоматически пытается вылечить все обнаруженные зараженные файлы. Если лечение невозможно, то эти файлы будут удалены; • «Лечить обнаруженные зараженные файлы» – приложение автоматически пытается вылечить все обнаруженные зараженные файлы; • «Удалять зараженные файлы» – приложение автоматически удаляет все обнаруженные зараженные файлы	Да
Режим сохранения событий в файл отчета	В шаблоне. Только для типа действия «Поиск	Поле для выбора режима сохранений событий в файл отчета. Доступны следующие значения для выбора: • «Критические события» – в файл отчета будет сохранена	Да

	вредоносного ПО»	информация только о критических событиях; • «Все события» – в файл отчета будет сохранена информация о всех событиях; • «Не сохранять события» – информация о событиях не сохраняется в файл отчета	
Выбрать Технологии проверки iChecker	В шаблоне. Только для типа действия «Поиск вредоносного ПО»	Поле для включения и выключения технологии iChecker, позволяющей ускорить проверку, исключая файлы по алгоритму с учетом даты баз, предыдущей проверки и настроек	Да
Область проверки	В шаблоне. Только для типа действия «Поиск вредоносного ПО»	Поле для выбора области проверки. Доступны следующие значения для выбора: • «Полная проверка. Kaspersky Endpoint Security» – проверка всех файлов, процессов и загрузочных областей компьютера; • «Проверить память ядра» – проверка оперативной памяти и системной области ядра ОС; • «Проверить объекты автозагрузки» – проверка реестра, планировщика заданий и папок «Автозагрузка»; • «Проверить почтовый ящик Outlook» – проверка файлов данных Outlook (OST\PST) и вложений писем; • «Проверить съемные диски» – проверка USB-накопителей, карты памяти и других съемных носителей; • «Проверить жесткие диски» – проверка всех внутренних жестких дисков компьютера; • «Проверить сетевые диски» – проверка подключенных сетевых дисков и UNC-путей;	Да

		• «Проверить файлы в резервном хранилище KES» – проверка объектов, находящихся в карантине Kaspersky Endpoint Security	
Технологии проверки iSwift	В шаблоне. Только для типа действия «Поиск вредоносного ПО»	Поле для включения и выключения технологии iSwift, позволяющей ускорить проверку, исключая файлы по алгоритму с учетом даты баз, предыдущей проверки и настроек	Да
Параметры обновления	В шаблоне. Только для типа действия «Обновление баз и модулей приложения»	Поле для выбора параметров обновления. Доступны следующие значения для выбора: • «Официальные сервера обновления» – запуск задачи «Обновление» с параметрами по умолчанию: источник обновления – серверы обновлений «Лаборатории Касперского»; • «Источники, указанные в политике» – запуск задачи «Обновление», созданной автоматически после установки (предустановленная задача); • «Указать источник обновления» – адрес HTTP-, FTP-сервера или папки общего доступа с пакетом обновлений. Допускается указание только одного источника	Да
Профиль	В шаблоне. Только для типа действий «Запуск профиля» и «Остановка профиля»	Поле для выбора профиля. Доступны следующие значения для выбора: • «Адаптивный контроль аномалий» – обнаружение подозрительной активности, отклоняющейся от нормального поведения системы; • «AMSI-защита» – интеграция с Windows Antimalware Scan Interface для блокировки	

		вредоносных скриптов и макросов; • «Анализ поведения» – отслеживание действий процессов в реальном времени для выявления вредоносного поведения; • «Контроль устройств» – управление доступом к USB, CD/DVD, Wi-Fi и другим периферийным устройствам; • «Контроль приложений» – ограничение запуска программ по категориям, репутации и правилам; • «Защита от файловых угроз» – постоянный мониторинг файлов на открытие, сохранение и выполнение; • «Сетевой экран» – фильтрация входящего и исходящего сетевого трафика по правилам; • «Предотвращение вторжений» – блокировка попыток эксплойта уязвимостей и несанкционированных действий; • «Защита от сетевых угроз» – обнаружение сетевых атак, порт-сканирования; и подозрительного трафика • «Проверка целостности» – контроль изменений критических системных файлов и реестра; • «Анализ журналов» – автоматический анализ событий ОС и приложений для выявления инцидентов; • «Защита от почтовых угроз» – проверка входящих и исходящих писем на вредоносные вложения и фишинг; • «Откат обновления» – возврат к предыдущей версии баз или	

		модулей при возникновении проблем; • «Фоновая проверка» – автоматическое сканирование при простое ПК для минимальной нагрузки; • «Проверка памяти ядра» – проверка оперативной памяти и системных областей на наличие вредоносного кода; • «Полная проверка» – глубокое сканирование всех дисков, памяти и загрузочных областей; • «Выборочная проверка» – проверка выбранных файлов, папок или дисков по требованию; • «Проверка объектов автозагрузки» – быстрая проверка объектов, загружаемых при запуске операционной системы; • «Проверка съемных дисков» – автоматическое или ручное сканирование USB-накопителей и карт памяти; • «Проверка важных областей» – проверка загрузочных секторов, памяти и автозагрузки на наличие активных угроз; • «Обновление» – загрузка и установка свежих антивирусных баз и программных модулей; • «Защита от веб-угроз» – блокировка вредоносных и фишинговых сайтов, проверка загружаемых файлов; • «Веб-Контроль» – фильтрация веб-контента по категориям и политикам безопасности	

4. СЦЕНАРИИ ДЛЯ ОС MACOS

4.1. Установка и удаление ПО

Код: SFT_MGMT_A

Сценарий предназначен для централизованной установки или удаления программного обеспечения на оконечных устройствах с ОС macOS.

4.1.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 30.

Таблица 30. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Действия	В шаблоне	Поле для выбора типа действия. Доступны выбор одного из двух вариантов: • «Установить указанное программное обеспечение» – запуск установки программного обеспечения, которое было выбрано в поле параметра «Инсталляционный пакет»; • «Удалить программное обеспечение» – запуск удаления программного обеспечения, которое было указано в поле параметра «Наименование программного обеспечения»	Да
Инсталляционный пакет	В шаблоне	Поле для выбора устанавливаемого программного обеспечения. Параметр доступен только при выборе значения «Установить указанное программное обеспечение» в параметре «Действия»	Да
Наименование программного обеспечения	В шаблоне	Поле для указания наименования удаляемого программного обеспечения. Параметр доступен только при выборе значения «Удалить программное обеспечение» в параметре «Действия»	Да

Отображение пропущенных задач	В задаче	Необходимость отображения пропущенных задач. Выбирается один из двух вариантов: • «Да» – пропущенные задачи будут отображены; • «Нет» – пропущенные задачи не будут отображены. Данное значение является значением по умолчанию	Нет

4.2. Запуск скриптов

Код: SE_SCRIPT_A

Сценарий предназначен для централизованного выполнения Bash-скриптов (.sh) скриптов на оконечных устройствах с ОС macOS. Поддерживает передачу аргументов командной строки и обеспечивает безопасное выполнение в изолированной рабочей среде.

4.2.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 31.

Таблица 31. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Файл скрипта	В шаблоне	Поле для выбора файла скрипта из списка. Поддерживаются файлы формата SH	Да
Аргументы запуска скрипта	В шаблоне	Поле для указания параметров командой строки для передачи скрипту	Нет

4.3. Доставка файла

Код: SE_FILE_A

Сценарий предназначен для централизованной доставки файлов на оконечные устройства под управлением ОС macOS. Позволяет копировать файлы в указанный каталог с возможностью переименования и автоматическим созданием необходимых директорий.

4.3.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 31.

Таблица 31. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Файл	В шаблоне	Поле для выбора файла, который будет доставлен на оконечные устройства	Да
Путь на оконечном устройстве	В шаблоне	Поле для указания пути на оконечном устройстве	Да

4.4. Управление учетными записями пользователей

Код: SEC_MGMT_USERS_A

Сценарий предназначен для управления учетными записями пользователей на оконечных устройствах под управлением ОС macOS. Позволяет централизованно проводить сброс паролей УЗ, добавлять УЗ в группы.

4.4.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 33.

Таблица 33. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Основное действие	В шаблоне	Поле для выбора совершаемого действия. Доступен выбор одного из следующих значений: • «Создать нового пользователя»; • «Сменить пароль пользователя»; • «Отключить возможность входа пользователю»; • «Добавить пользователя в локальную группу»; • «Удалить пользователя из локальной группы»	Да
Имя пользователя	В шаблоне	Поле для указания имени УЗ, которое должно состоять из строчных латинских букв (a-z), цифр (0-9) и дефисов (-). Имя должно начинаться с буквы. Пример: user-name	Да

Полное имя пользователя	В шаблоне	Поле для указания отображаемого имени УЗ. Может содержать кириллицу, латиницу, пробелы и специальные символы	Да
Пользователь (из списка)	В шаблоне	Поле для выбора пользователя из списка доступных учетных записей системы	Да
Локальная группа	В шаблоне	Поле для выбора локальной группы из списка доступных групп системы	Да
Пароль пользователя	В задаче	Поле для указания пароля от УЗ. Пароль должен соответствовать политике безопасности системы, включая минимальную длину, требования к сложности и другие ограничения	Да

4.5. Управление профилями Cisco AnyConnect

Код: SFT_MGMT_CISCO_AC_A

Сценарий предназначен для централизованного управления профилями VPN-подключений Cisco AnyConnect Secure Mobility Client на оконечных устройствах с ОС Windows. Позволяет добавлять и удалять XML-профили конфигурации с автоматической перезагрузкой служб.

Параметры и примеры использования сценария совпадают с параметрами и примерами для ОС Windows (см. подраздел 3.4 настоящего руководства).

4.6. Переименование устройства

Код: SYS_HOSNTAME_A

Сценарий предназначен для автоматического переименования устройств по заданной политике именования. Система проверяет соответствие имен устройств настроенной политике именования. В случае несоответствия генерирует уникальные имена на основе префикса и числовой последовательности, ведет учет назначенных имен и предотвращает конфликты имен в сети.

Параметры и примеры использования сценария совпадают с параметрами и примерами для ОС Windows (см. подраздел 3.14 настоящего руководства).

4.7. Добавление устройства в домен

Код: SEC_MGMT_AD_A

Сценарий предназначен для автоматического добавления оконечных устройств под управлением ОС Windows в домен Active Directory (AD). Сценарий автоматически находит свободное имя компьютера в заданном диапазоне, добавляет устройство в указанную организационную единицу (OU) домена и выполняет перезагрузку для применения изменений.

Параметры и примеры использования сценария совпадают с параметрами и примерами для ОС Windows (см. подраздел 3.15 настоящего руководства).

4.8. Управление профилями КриптоПро Ngate

Код: MGMT_NGATE_A

Сценарий предназначен для централизованного управления агентом КриптоПро NGate на оконечных устройствах под управлением ОС macOS.

4.8.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 34.

Таблица 34. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Основное действие	В шаблоне	Поле для выбора типа клиента, для которого будет выполнена настройка конфигурационного файла. Выбирается один из следующих вариантов: • «Настройка конфигурационного файла графического клиента» – изменение настроек конфигурации для графического клиента; • «Настройка конфигурационного файла консольного клиента» – изменение настроек конфигурации для консольного клиента	Да
Действие	В шаблоне	Поле доступно только при выборе в поле «Основное действие» варианта «Настройка конфигурационного файла графического клиента». В данном поле	Да

		необходимо выбрать выполняемое действие: • «Добавить новое подключение»; • «Изменить существующее подключение»; • «Удалить существующее подключение»	
Настроить глобальные параметры	В шаблоне	Поле доступно только при выборе в поле «Основное действие» варианта «Настройка конфигурационного файла графического клиента». В данном поле указывается необходимость настройки глобальных параметров. Для этого требуется выбрать один из вариантов: • «Да, настроить»; • «Нет, не настраивать»	Да
Новый адрес шлюза	В шаблоне	Поле для указания адреса шлюза в формате FQDN. Поле доступно только при выборе действий «Изменить существующее подключение» или «Добавить новое подключение»	Нет
Текущий адрес шлюза	В шаблоне	Поле для указания адреса шлюза в формате FQDN, которое будет изменено или удалено. Поле доступно только при выборе действий «Изменить существующее подключение» или «Удалить существующее подключение»	Нет
Тип подключения	В шаблоне	Поле доступно только при выборе в поле «Основное действие» варианта «Настройка конфигурационного файла консольного клиента». В данном поле необходимо выбрать тип подключения: • «Подключение на основе логин/пароля»; • «Подключение на основе сертификата»	Да
Адрес шлюза	В шаблоне	Поле доступно только при выборе в поле «Основное действие» варианта «Настройка конфигурационного файла консольного клиента». В данном поле необходимо указать отпечаток	Нет

		сертификата в шестнадцатеричном формате	
Имя сертификата	В шаблоне	Поле доступно только при выборе типа подключения «Подключение на основе сертификата». В данном поле необходимо указать имя сертификата (certificateCommonName)	Нет
Отпечаток сертификата	В шаблоне	Поле доступно только при выборе типа подключения «Подключение на основе сертификата». В данном поле необходимо указать отпечаток сертификата	Нет

5. СЦЕНАРИИ ДЛЯ ОС LINUX

5.1. Добавление устройства в домен

Код: SEC_MGMT_AD_L

Сценарий предназначен для автоматического добавления оконечных устройств под управлением ОС Linux. Сценарий автоматически находит свободное имя компьютера в заданном диапазоне, добавляет устройство в указанную организационную единицу (OU) домена и выполняет перезагрузку для применения изменений.

5.1.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 35.

Таблица 35. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Действие	В шаблоне	Поле для выбора способа добавления компьютера в домен. Выбирается один из двух способов: • «Добавление в домен с текущим именем» – компьютер будет добавлен в домен с использованием текущего имени; • «Добавление в домен с новым именем» – при добавлении в домен будет использовано новое имя	Да
Имя домена	В шаблоне	Поле для указания имени компьютера	Да
Организационная единица (OU)	В шаблоне	Поле для указания наименования организационной единицы	Да
Способ генерации нового имени	В шаблоне	Поле для выбора способа генерации нового имени компьютер. Выбирается один из двух способов: • «Найти первое свободное имя в OU» – будет использовано первое свободное в	Да

		организационной единице уникальное имя; • «Найти первое свободное имя в OU (в указанном диапазоне)» – будет использовано первое свободное в организационной единице уникальное имя в заданном диапазоне. Поле доступно только при выборе действия «Добавление в домен с новым именем»	
Префикс нового имени	В шаблоне	Поле для указания префикса для имени компьютера, к которому автоматически будет добавлен сгенерированный номер. Поле доступно только при выборе действия «Добавление в домен с новым именем»	Да
Начальное значение диапазона	В шаблоне	Поле для указания максимального значения в диапазоне для автоматической генерации имени компьютера. Поле доступно только при выборе действия «Добавление в домен с новым именем» и способа генерации «Найти первое свободное имя в OU (в указанном диапазоне)»	Да
Конечное значение диапазона	В шаблоне	Поле для указания минимального значения в диапазоне для автоматической генерации имени домена. Поле доступно только при выборе действия «Добавление в домен с новым именем» и способа генерации «Найти первое свободное имя в OU (в указанном диапазоне)»	Да
Логин администратора домена	В задаче	Поле для указания имени пользователя технической учетной записи (ТУЗ) с правами добавления компьютеров в домен	Да

Пароль администратора домена	В задаче	Поле для указания пароля от технической учетной записи	Да
Отображение пропущенных задач	В задаче	Необходимость отображения пропущенных задач. Выбирается один из двух вариантов: • «Да» – пропущенные задачи будут отображены; • «Нет» – пропущенные задачи не будут отображены. Данное значение является значением по умолчанию	Нет

5.2. Установка SSL\TLS сертификатов

Код: SEC_MGMT_CERT_L

Сценарий предназначен для централизованной установки SSL\TLS сертификатов в хранилища ОС Linux на оконечных устройствах. Позволяет автоматически развертывать корневые сертификаты, промежуточные сертификаты центров сертификации и пользовательские сертификаты в соответствующие системные хранилища.

5.2.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 36.

Таблица 36. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Файл сертификата	В шаблоне	Поле для выбора файла с сертификатами. Допускается загрузка файлов формата CRT и PEM	Нет
Имя сертификата	В шаблоне	Поле для указания наименования сертификата (без использования пробелов)	Да

5.3. Запуск скриптов

Код: SE_SCRIPT_ L

Сценарий предназначен для централизованного выполнения Shell (.sh) и пакетных (.bat/.cmd) скриптов на оконечных устройствах с ОС Linux. Поддерживает передачу аргументов командной строки и обеспечивает безопасное выполнение в изолированной рабочей среде.

5.3.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 37.

Таблица 37. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Файл скрипта	В шаблоне	Поле для выбора файла скрипта из списка. Поддерживаются файлы формата SH, BAT и CMD	Да
Аргументы запуска скрипта	В шаблоне	Поле для указания параметров командой строки для передачи скрипту	Нет

5.4. Установка и удаление ПО

Код: SFT_MGMT_L

Сценарий предназначен для централизованной установки или удаления программного обеспечения на оконечных устройствах с ОС Linux.

5.4.1. Параметры сценария

Состав и описание параметров, включая место и обязательность заполнения, представлен в таблице 38.

Таблица 38. Состав и описание параметров сценария

Название параметра	Место заполнения	Описание	Обязательность
Инсталляционный пакет	В шаблоне	Поле для выбора файла программного обеспечения для установки. Поддерживаются файлы формата DEB и RPM. Параметр указывается только при выборе действия «Установить указанный пакет»	Нет

Действие	В шаблоне	Поле для выбора действия с программным обеспечением. Выбирается один из следующих вариантов: • «Установить программное обеспечение из репозитория» – будет выполнена установка программного обеспечения из настроенных репозиториев операционной системы; • «Установить указанный пакет» – будет выполнена установка пакета программного обеспечения, указанного в графе «Инсталляционный пакет»; • «Удалить программное обеспечение» – будет выполнено удаление программного обеспечения; • «Обновить программное обеспечение из репозитория» – будет выполнено обновление программного обеспечения из настроенных репозиториев операционной системы	Да
Наименование программного обеспечения	В шаблоне	Поле для указания наименования программного обеспечения, с которым будет выполнено выбранное действие	Нет
Отображение пропущенных задач	В задаче	Необходимость отображения пропущенных задач. Выбирается один из двух вариантов: • «Да» – пропущенные задачи будут отображены; • «Нет» – пропущенные задачи не будут отображены. Данное значение является значением по умолчанию	Нет