

Описание стенда Secret Net Studio

Оглавление

Описание сетевой структуры и виртуальных машин стенда	1
Сценарии использования	13
Сценарий №1 "Установка компонентов Secret Net Studio в сетевом варианте".....	13
Сценарий №2 "Локальная настройка Secret Net Studio в соответствии с заданными параметрами"	31
Сценарий №3 "Настройка механизма контроля целостности"	36
Сценарий №4 "Централизованное ведение журналов в Secret Net Studio"	47
Сценарий №5 "Управление подчинением защищаемых компьютеров серверу безопасности SNS"	67
Сценарий №6 "Настройка полномочного управления доступом"	74
Сценарий №7 "Настройка механизма дискреционного управления доступом"	83
Сценарий №8 "Управление доступом к съемным носителям информации"	89
Сценарий №9 "Настройка механизма замкнутой программной среды"	100
Сценарий №10 "Персональный межсетевой экран"	110
Сценарий №11 "Авторизация сетевых соединений"	123
Сценарий №12 "Настройка антивируса и COB"	131

Описание сетевой структуры и виртуальных машин стенда

Для выполнения сценариев подготовлен специальный тестовый стенд на платформе VMware vSphere из 6 виртуальных машин с установленными операционными системами.

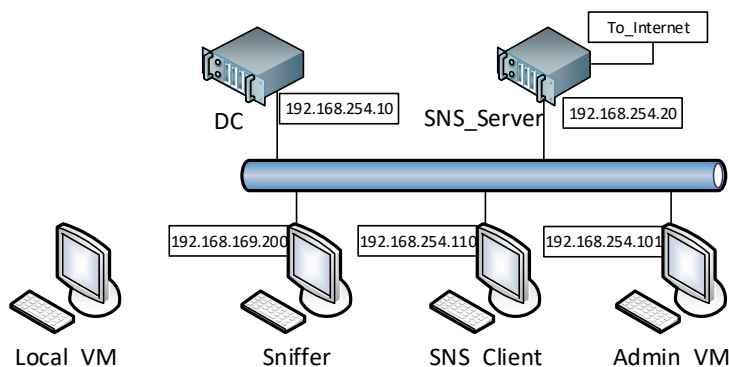


Рис. 1. Схема стенда Secret Net Studio

Стенд построен на виртуальной локальной сети 192.168.254.X/24, объединяющей 4 виртуальные машины. VM Sniffer для перехвата сетевого трафика имеет сетевой интерфейс, подключенный к отдельному виртуальному коммутатору в режиме Promiscuous mode, с IP-адресом другой подсети.

Одна VM – Local_VM – является отдельной и не включена в виртуальную сеть.

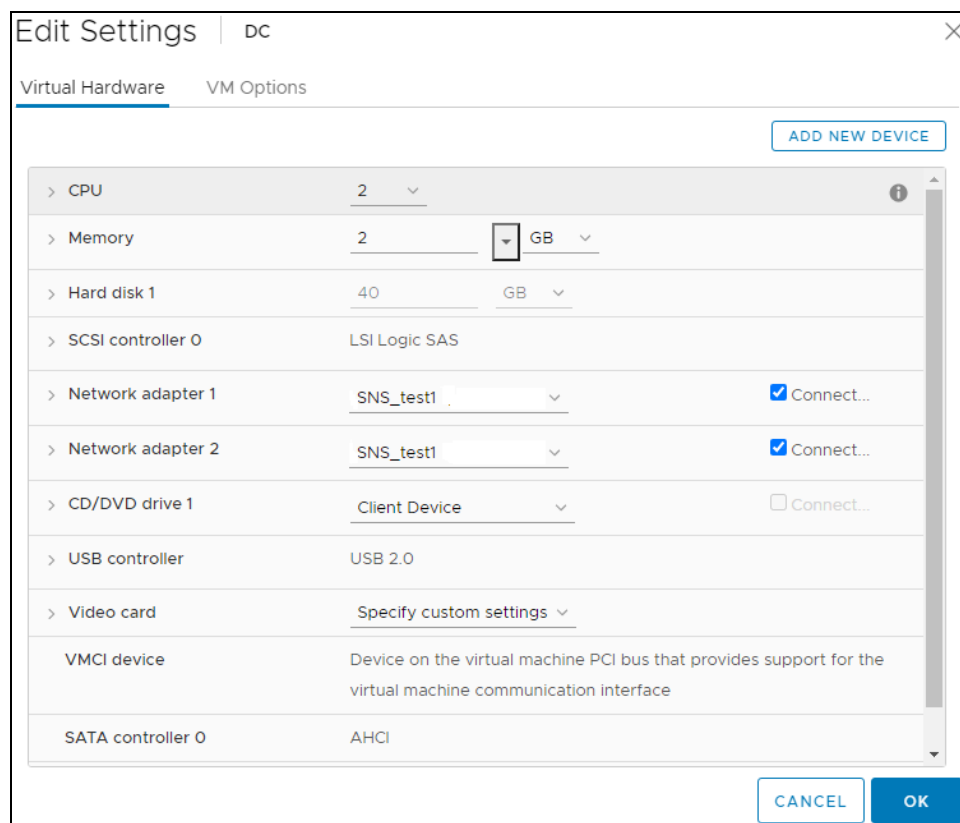
Ниже приводится описание всех VM стенда.

Внимание! При подготовке с нуля аналогичного стенда его можно разворачивать в этом же порядке.

Для всех VM стенда выбрана совместимость (compatibility): ESXi 6.5 and later (VM version 13).

VM **DC** выполняет функции контроллера домена **domain1.local** и имеет следующие характеристики:

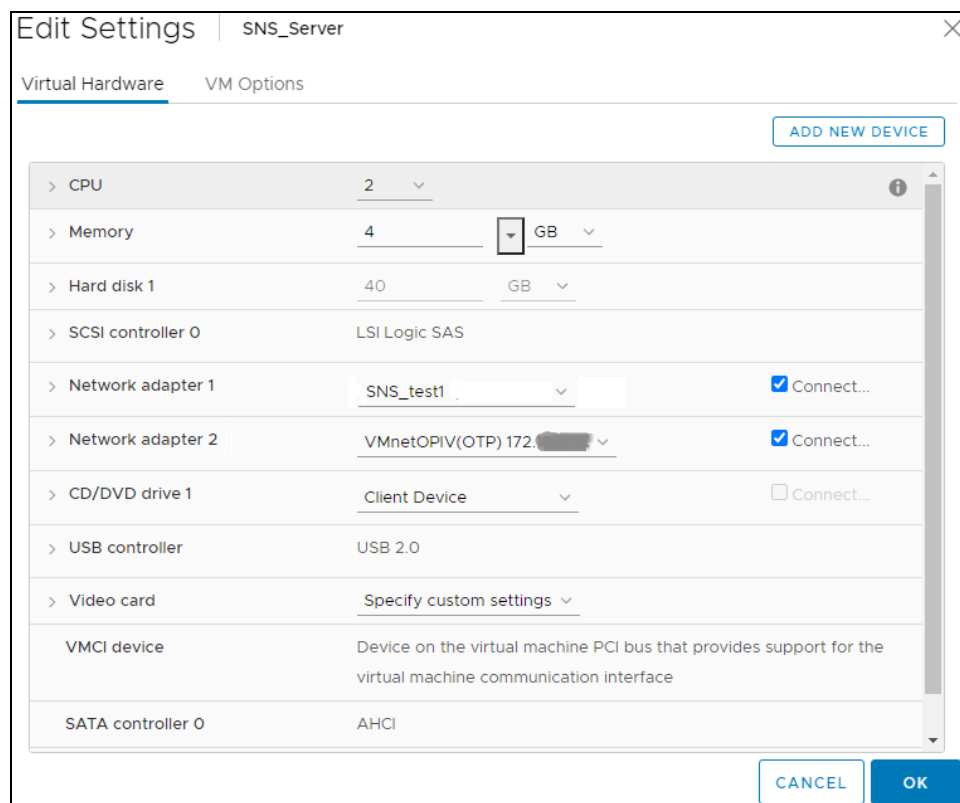
- "Guest Operating System" – "Windows", "Version" – "Microsoft Windows Server 2012 (64-bit)";
- аппаратные характеристики VM: memory – 2ГБ, CPUs: virtual socket – 1, cores per socket – 2; hard disk 1 – 40ГБ (Thin Provision), USB-controller, network adapters – 2 (E1000E);



- установлена ОС Microsoft Windows Server 2012 R2 Standard (64-bit). Прописаны следующие параметры сетевых интерфейсов:
 - 1-й сетевой интерфейс: IP-адрес – **192.168.254.10**, маска – **255.255.255.0**, DNS-сервер – **127.0.0.1**. Отключен протокол IPv6;
 - 2-й сетевой интерфейс не используется;
- встроенная локальная УЗ администратора: логин – **Администратор**, пароль – **P@ssw0rd**;
- установлены роли: "DNS-сервер", "Доменные службы Active Directory" и "Службы Active Directory облегченного доступа к каталогам (AD LDS)". Наименование домена – **domain1.local**;
- дополнительная доменная УЗ администратора домена безопасности SNS: логин – **snsadmin**, пароль – **P@ssw0rd**;
- пользовательские доменные учетные записи **"user1 – Иванов Иван Иванович"** и **"user2 – Петров Петр Петрович"** с паролем **P@ssw0rd**;
- установлен пакет обновлений KB2999226;
- выключены UAC и брандмауэр Windows.

ВМ **SNS_Server** выполняет функции сервера безопасности Secret Net Studio в составе домена **domain1.local** и имеет следующие характеристики:

- "Guest Operating System" – "Windows", "Version" – "Microsoft Windows Server 2012 (64-bit)";
- аппаратные характеристики ВМ: memory – 4ГБ, CPUs: virtual socket – 1, cores per socket – 2; hard disk 1 – 40ГБ (Thin Provision), USB-controller, network adapters – 2 (VMXNET 3), firmware boot option – EFI;



- установлена ОС Microsoft Windows Server 2012 R2 Standard (64-bit). Прописаны следующие параметры сетевых интерфейсов:
 - 1-й сетевой интерфейс: IP-адрес – **192.168.254.20**, маска – **255.255.255.0**, DNS-сервер – **192.168.254.10**. Отключен протокол IPv6;
 - 2-й сетевой интерфейс следует настроить для обеспечения взаимодействия с сервером обновлений компании "Код Безопасности" (<https://updates.securitycode.ru:43444>) и в свойствах сетевого соединения выключить протокол IPv6;
- встроенная локальная УЗ администратора: логин – **Администратор**, пароль – **P@ssw0rd**;
- установлен пакет обновлений KB2999226;
- установлен компонент .NET Framework 3.5;
- компьютер зарегистрирован в домене **domain1.local**;
- установлены telnet-сервер и клиент;
- установлено разрешение подключения к удаленному рабочему столу для всех сетевых подключений на этом компьютере. Доменные пользователи "domain1\snsadmin", "domain1\user1" и "domain1\user2" включены в локальную группу "Пользователи удаленного рабочего стола" ("Remote Desktop Users");
- на локальном диске в папке "C:\Distrib" размещено необходимое ПО для установки;
- выключены UAC и брандмауэр Windows.

ВМ **Admin_VM** выполняет функции рабочего места администратора безопасности в составе домена **domain1.local** и имеет следующие характеристики:

- "Guest Operating System" – "Windows", "Version" – "Microsoft Windows 10 (64-bit)";
- аппаратные характеристики ВМ: memory – 4ГБ, CPUs: virtual socket – 1, cores per socket – 2, установлены параметры "Expose hardware assisted virtualization to the guest OS" и "Enable virtualized CPU performance counters"; hard disk 1 – 40ГБ (Thin Provision), USB-controller (USB 2.0), network adapters – 2 (E1000E), firmware boot option – EFI;

Edit Settings | Admin_VM

Virtual Hardware | VM Options

ADD NEW DEVICE

CPU	2	
Cores per Socket	2	Sockets: 1
CPU Hot Plug	☐ Enable CPU Hot Add	
Reservation	0	MHz
Limit	Unlimited	MHz
Shares	Normal	2000
CPUID Mask	Expose the NX/XD flag to guest Advanced...	
Hardware virtualization	☒ Expose hardware assisted virtualization to the guest OS	
Performance Counters	☒ Enable virtualized CPU performance counters	
CPU/MMU Virtualization	Automatic	
Memory	4	GB
Hard disk 1	40	GB

CANCEL OK

Memory	4	GB
Hard disk 1	40	GB
SCSI controller 0	LSI Logic SAS	
Network adapter 1	SNS_test1	☒ Connect...
Network adapter 2	SNS_test1	☒ Connect...
CD/DVD drive 1	Client Device	☐ Connect...
USB controller	USB 2.0	
Video card	Specify custom settings	
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface	
SATA controller 0	AHCI	
Other	Additional Hardware	

CANCEL OK

- установлена ОС Microsoft Windows 10 21H1 (64-bit). Прописаны следующие параметры сетевых интерфейсов:
 - 1-й сетевой интерфейс: IP-адрес – **192.168.254.101**, маска – **255.255.255.0**, DNS-сервер – **192.168.254.10**. Отключен протокол IPv6;
 - 2-й сетевой интерфейс не используется;
- встроенная локальная УЗ администратора: логин – **admin**, пароль – **P@ssw0rd**;
- компьютер зарегистрирован в домене **domain1.local**;
- установлен пакет Microsoft Office 2013;
- установлен telnet-клиент;
- выключены UAC и брандмауэр Windows;

- на локальном диске "C:\\" в папке "Distrib" размещено необходимое ПО.

ВМ **SNS_Client** выполняет функции защищаемого клиентского компьютера в составе домена **domain1.local** и имеет следующие характеристики:

- "Guest Operating System" – "Windows", "Version" – "Microsoft Windows 10 (64-bit)";
- аппаратные характеристики ВМ: memory – 2ГБ, CPUs: virtual socket – 1, cores per socket – 2, установлен параметр "Expose hardware assisted virtualization to the guest OS"; hard disk 1 – 40ГБ (Thin Provision), USB-controller (USB 2.0), network adapters – 1 (E1000E), firmware boot option – EFI;

Edit Settings | SNS_Client

Virtual Hardware VM Options

ADD NEW DEVICE

CPU	2	
Cores per Socket	2	Sockets: 1
CPU Hot Plug	☐ Enable CPU Hot Add	
Reservation	0	MHz
Limit	Unlimited	MHz
Shares	Normal	2000
CPUID Mask	Expose the NX/XD flag to guest Advanced...	
Hardware virtualization	☒ Expose hardware assisted virtualization to the guest OS	
Performance Counters	☐ Enable virtualized CPU performance counters	
CPU/MMU Virtualization	Automatic	
Memory	2	GB
Hard disk 1	40	GB

CANCEL OK

Edit Settings | SNS_Client

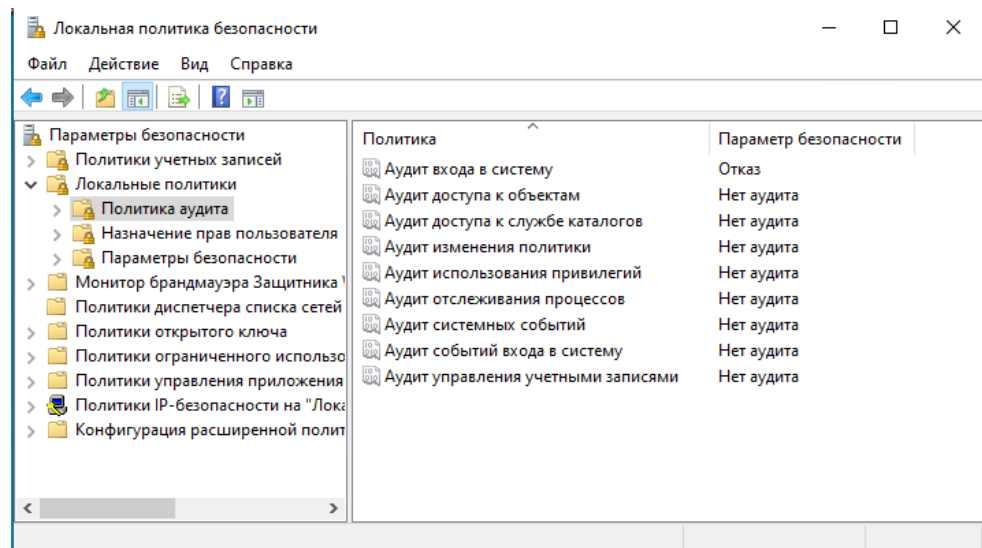
Virtual Hardware VM Options

ADD NEW DEVICE

CPU	2	
Memory	2	GB
Hard disk 1	40	GB
SCSI controller 0	LSI Logic SAS	
Network adapter 1	SNS_test1	☒ Connect...
CD/DVD drive 1	Client Device	☐ Connect...
USB controller	USB 2.0	
Video card	Specify custom settings	
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface	
SATA controller 0	AHCI	

CANCEL OK

- установлена ОС Microsoft Windows 10 21H1 (64-bit). Прописаны следующие параметры сетевого интерфейса: IP-адрес – **192.168.254.110**, маска – **255.255.255.0**, DNS-сервер – **192.168.254.10**. Отключен протокол IPv6;
- встроенная локальная УЗ администратора: логин – **admin**, пароль – **P@ssw0rd**;
- компьютер зарегистрирован в домене **domain1.local**;
- установлен пакет Microsoft Office 2013;
- на локальном диске в папке "C:\Distrib" размещено необходимое ПО;
- установлен telnet-клиент;
- в локальной политике безопасности Windows включен аудит отказов попыток входа в систему;



- в реестре Windows установлен параметр: HKLM / SYSTEM / CCS / services / Tcpip / Parameters / IpEnableRouter – 1;
- выключены UAC и брандмауэр Windows.

ВМ **Local_VM** выполняет функции отдельного защищаемого компьютера и имеет следующие характеристики:

- "Guest Operating System" – "Windows", "Version" – "Microsoft Windows 10 (64-bit)";
- аппаратные характеристики ВМ: memory – 4ГБ, CPUs: virtual socket – 1, cores per socket – 2, установлен параметр "Expose hardware assisted virtualization to the guest OS"; hard disk 1 – 40ГБ (Thin Provision), USB-controller (USB 2.0), network adapters – 1 (E1000E), firmware boot option – EFI;

Edit Settings | Local_VM

Virtual Hardware VM Options

ADD NEW DEVICE

CPU	2		
Cores per Socket	2	Sockets: 1	
CPU Hot Plug	☐ Enable CPU Hot Add		
Reservation	0	MHz	
Limit	Unlimited	MHz	
Shares	Normal	2000	
CPUID Mask	Expose the NX/XD flag to guest Advanced...		
Hardware virtualization	☒ Expose hardware assisted virtualization to the guest OS		
Performance Counters	☐ Enable virtualized CPU performance counters		
CPU/MMU Virtualization	Automatic		
Memory	4	GB	
Hard disk 1	40	GB	

CANCEL OK

Edit Settings | Local_VM

Virtual Hardware VM Options

ADD NEW DEVICE

CPU	2		
Memory	4	GB	
Hard disk 1	40	GB	
SCSI controller 0	LSI Logic SAS		
Network adapter 1	SNS_test1		☒ Connect...
CD/DVD drive 1	Client Device		☐ Connect...
USB controller	USB 2.0		
Video card	Specify custom settings		
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface		
SATA controller 0	AHCI		
Other	Additional Hardware		

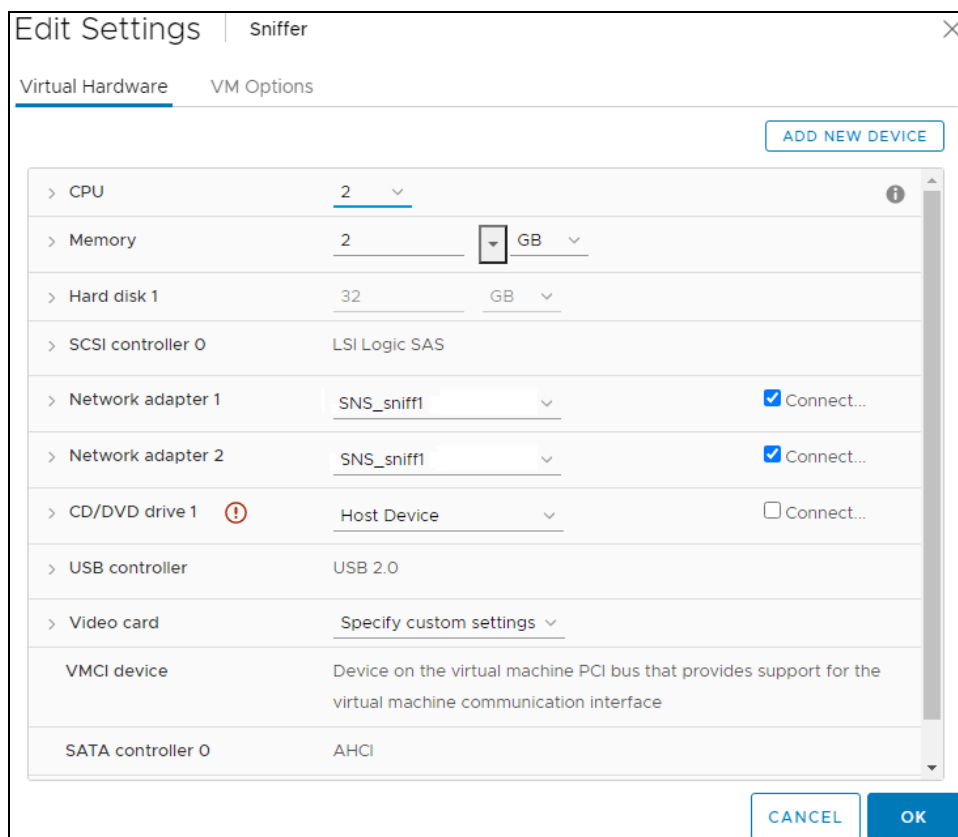
CANCEL OK

- установлена ОС Microsoft Windows 10 21H1 (64-bit);
- встроенная УЗ с правами локального администратора: логин – **admin**, пароль – **P@ssw0rd**;
- установлен пакет Microsoft Office 2013;
- на локальном диске в папке "C:\Distrib" размещено необходимое ПО для установки;

- локальные пользовательские УЗ: логин – **"user1 – Иванов Иван Иванович"** и **"user2 – Петров Петр Петрович"**, пароль – **P@ssw0rd**;
- выключены UAC и брандмауэр Windows.

ВМ **Sniffer** выполняет функции рабочего места для перехвата сетевого трафика и имеет следующие характеристики:

- "Guest Operating System" – "Windows", "Version" – "Microsoft Windows 10 (64-bit)";
- аппаратные характеристики ВМ: memory – 2ГБ, CPUs: virtual sockets – 1, cores per socket – 2; hard disk 1 – 32ГБ (Thin Provision), USB-controller (USB 2.0), network adapters – 2 (E1000E), один из которых подключен к виртуальному коммутатору, работающему в режиме Promiscuous mode для перехвата сетевого трафика, а второй не используется; firmware boot option – EFI;



- установлена ОС Microsoft Windows 10 21H1 (64-bit). Прописаны следующие параметры сетевых интерфейсов:
 - 1-й сетевой интерфейс: IP-адрес – **192.168.169.200**, маска – **255.255.255.0**. Отключен протокол IPv6;
 - 2-й сетевой интерфейс не используется;
- встроенная локальная УЗ администратора: логин – **admin**, пароль – **P@ssw0rd**;
- установлен Wireshark 2.0.2 (64-bit) for Windows;
- на локальном диске в папке "C:\Distrib" размещено необходимое ПО;
- выключены UAC и брандмауэр Windows.

Перед началом работы стенд следует развернуть в структуре VMware vSphere с использованием файл-образов, которые предоставляются вместе с методическими материалами.

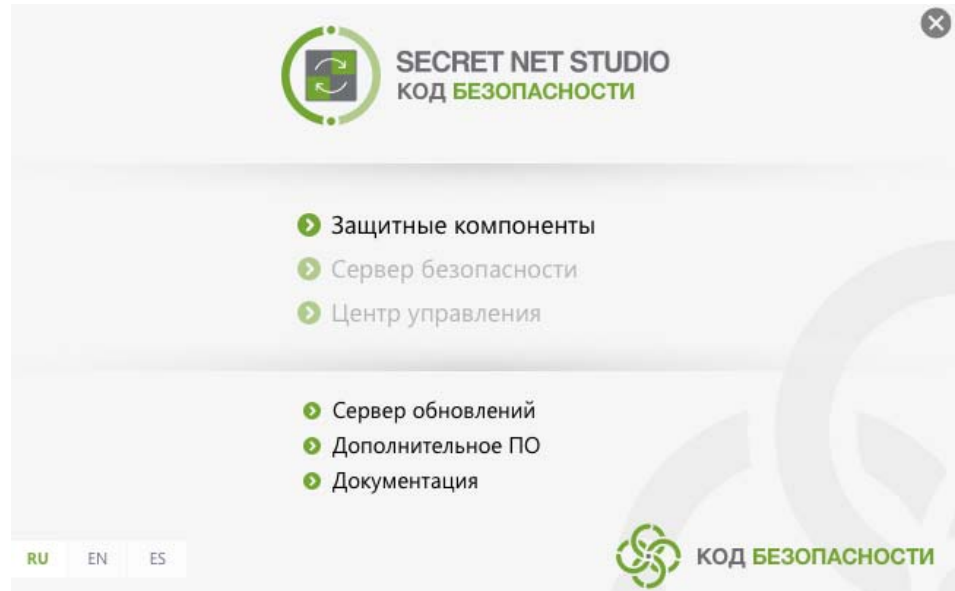
С помощью утилиты **ping** убедитесь, что с ВМ Admin_VM и SNS_Client есть взаимодействие с ВМ SNS_Server. Если это не так, убедитесь, что на всех ВМ отключен брандмауэр Windows.

На стенде используется СЗИ Secret Net Studio версии 8.8.

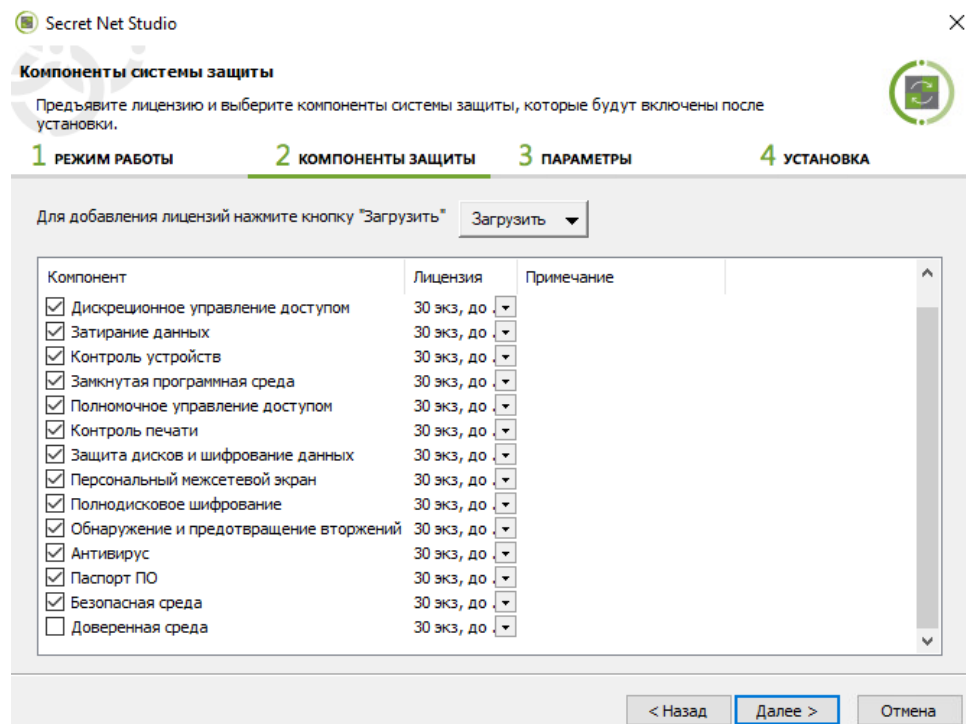


Далее приводится описание подготовительных операций, которые необходимо провести до начала работы со стендом.

1. На VM Local-VM авторизуйтесь под учетной записью локального администратора "admin" с паролем "P@ssw0rd". Из папки "C:\Distrib\SNS_8_8_XXXX" запустите файл SnAutoRun.exe и проведите автономную установку клиента Secret Net Studio. При этом:
 - выберите вариант установки "Защитные компоненты" и в процессе установки используйте параметры по умолчанию;

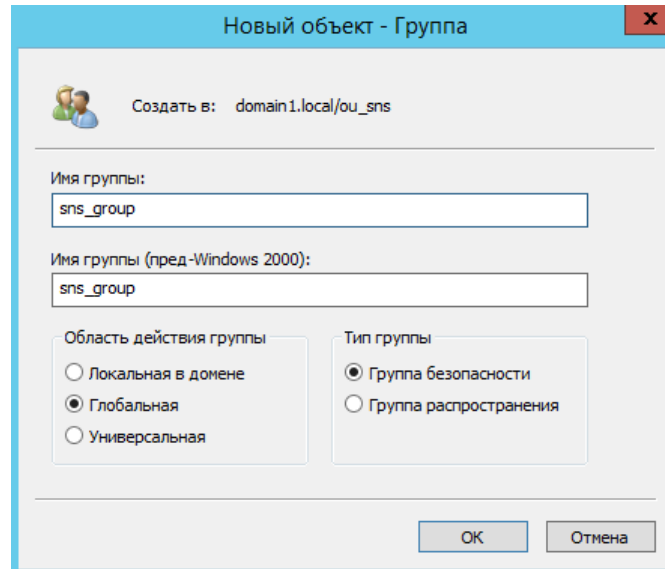


- на этапе выбора лицензии убедитесь, что выбран переключатель "ввести новую лицензию", нажмите кнопку "Выбрать" и выберите из папки "C:\Distrib" файл с полной лицензией. Поскольку компонент "Доверенная среда" может использоваться только на физическом компьютере и не активируется в виртуальной среде – снимите соответствующий флажок в списке компонентов;

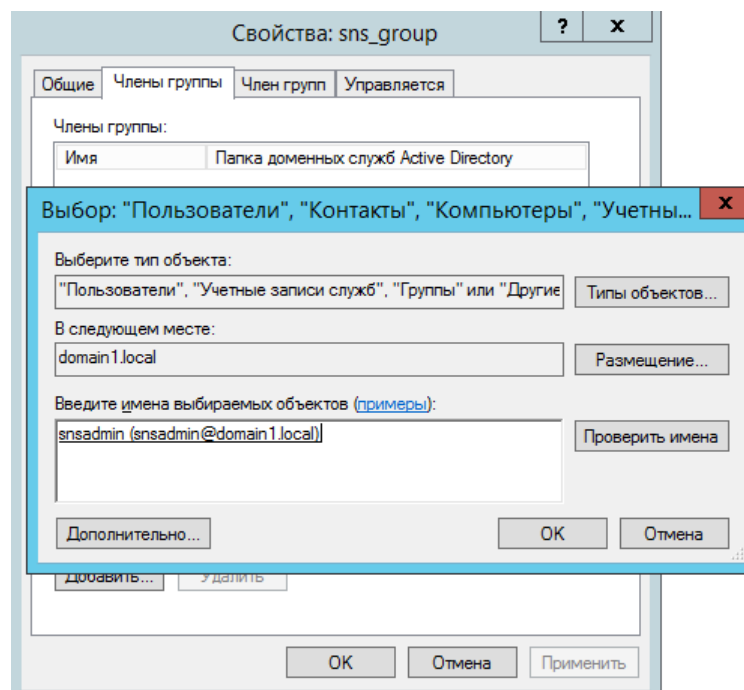


- после завершения установки перезагрузите VM Local-VM.
2. В домене "domain1.local" выполните подготовительные действия для установки Secret Net Studio в сетевом варианте:

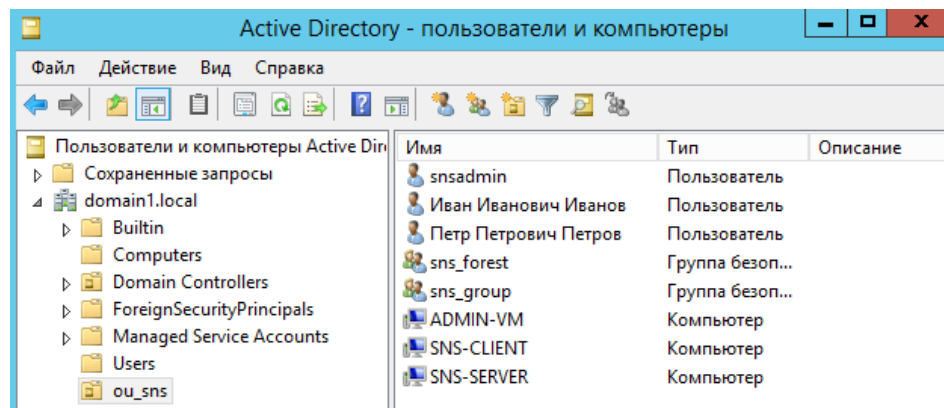
- создайте организационное подразделение "ou_sns", на базе которого будет формироваться домен безопасности Secret Net Studio;
- пользователей будущего домена безопасности "snsadmin", "user1" ("Иван Иванович Иванов") и "user2" ("Петр Петрович Петров") включите в состав организационного подразделения "ou_sns";
- в составе организационного подразделения "ou_sns" создайте группы пользователей: "sns_forest" – группу администраторов леса доменов безопасности и "sns_group" – группу администраторов домена безопасности;



- включите пользователя "snsadmin" в группы безопасности "sns_forest" и "sns_group". Для этого последовательно откройте окно свойств каждой из групп и во вкладке "Члены группы" ("Members") добавьте пользователя "snsadmin" домена "domain1.local" в группу;

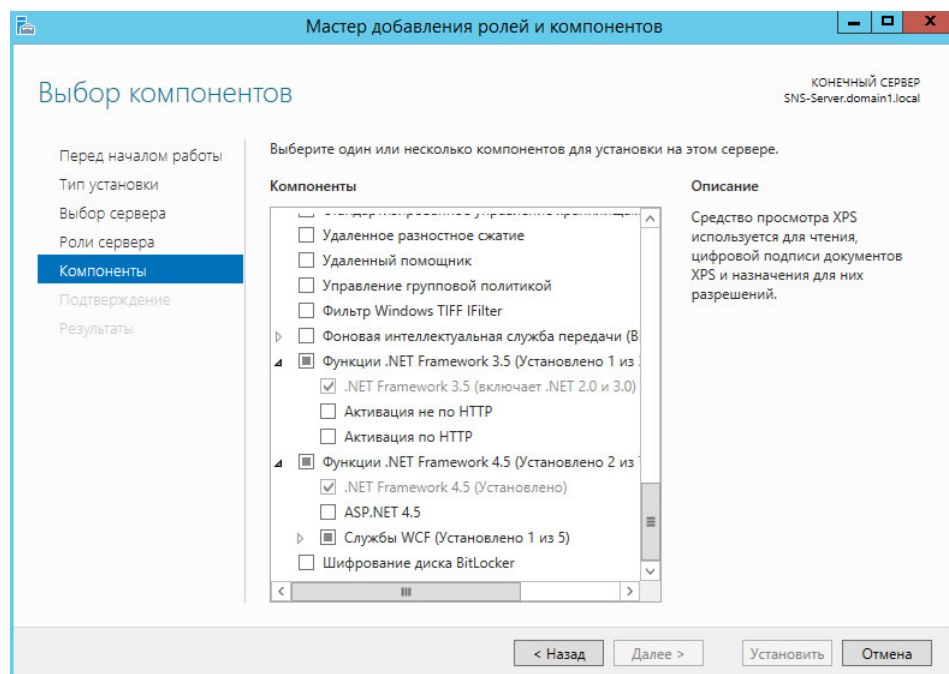


- переместите в подразделение "ou_sns" компьютеры, которые будут входить в домен безопасности Secret Net Studio: SNS-Server, SNS-Client и Admin-VM. Сформированная в итоге структура участников домена безопасности Secret Net Studio представлена на рисунке.

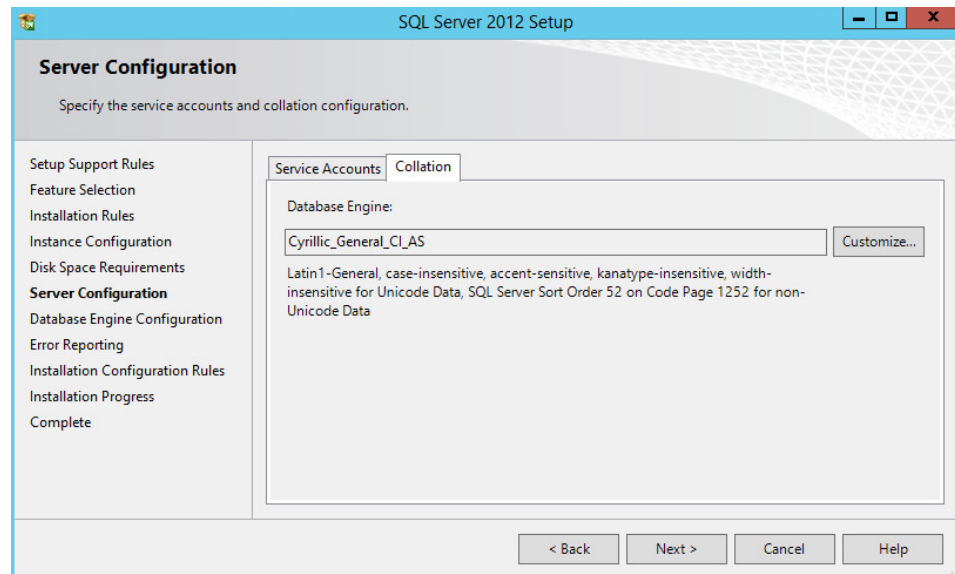


3. На компьютере сервера безопасности SNS-Server сделайте следующее:

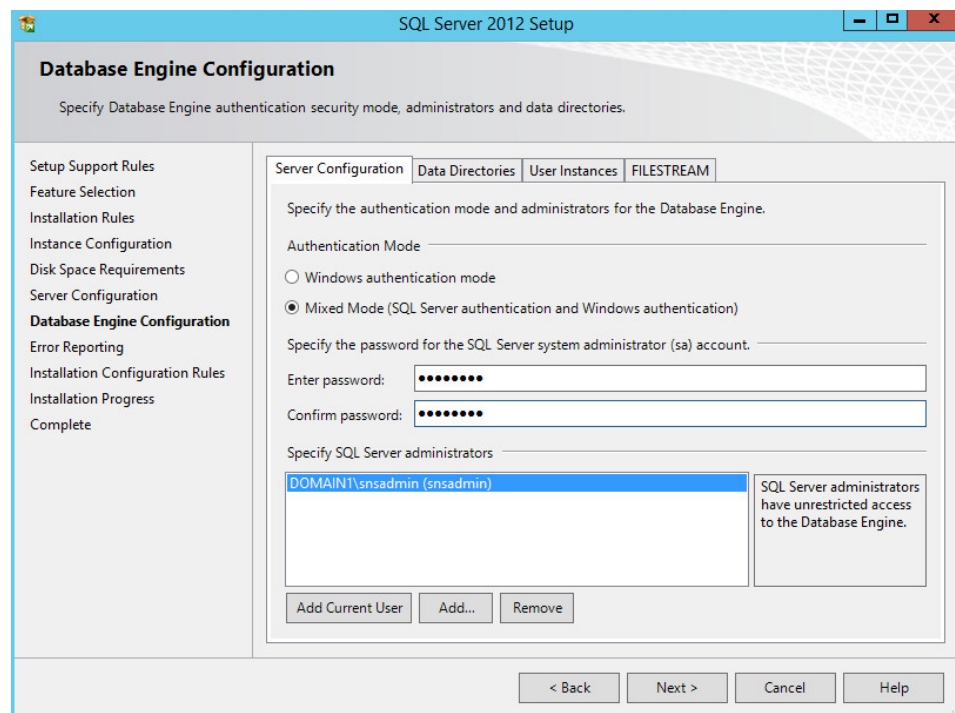
- под учетной записью администратора домена включите доменную группу "sns_group" в группу локальных администраторов данного сервера. После этого переавторизуйтесь в ОС с учетной записью "domain1\snsadmin" с паролем "P@ssw0rd";
- убедитесь, что в ОС Windows установлены компоненты .NET Framework версий 3.5 и 4.5;



- установите сервер MS SQL. Для этого из папки "C:\Distrib\" запустите файл "SQLEXPRT_x64_ENU.exe", дождитесь завершения выполнения мастером установки подготовительных действий и в разделе "Installation" выберите вариант новой установки отдельного SQL-сервера "New SQL Server stand-alone installation...";
- в ходе дальнейшей установки в основном следуйте указаниям мастера. При этом для обеспечения корректного взаимодействия сервера безопасности и СУБД MS SQL следует аккуратно установить перечисленные ниже опции;
- в категории параметров "Server Configuration" на вкладке "Collation" убедитесь, что включен режим поддержки сортировки кириллицы для экземпляра базы данных – в параметрах сортировки для компонента Database Engine установлено значение "Cyrillic_General_CI_AS";



- в категории параметров "Database Engine Configuration" необходимо включить смешанный режим аутентификации (mixed mode) – на вкладке "Server Configuration" установите переключатель "Mixed Mode (SQL Server authentication and Windows authentication)". Убедитесь, что в поле "Specify SQL Server administrators" присутствует доменная запись "snsadmin" и в полях "Enter password" и "Confirm password" введите пароль администратора SQL (sa) – **P@ssw0rd**;



- в категории "Database Engine Configuration" желательно включить группу локальных администраторов компьютера в группу администраторов SQL-сервера ("Specify SQL Server administrators") – добавьте группу "BUILTIN\Администраторы" ("BUILTIN\Administrators");

- нажмите кнопку "Next" и, следуя указаниям мастера, доведите процедуру установки до конца, перезагрузите BM SNS-Server и авторизуйтесь под учетной записью "domain1\snsadmin" с паролем "P@ssw0rd".
- 4. На BM SNS_Client и Admin_VM сделайте следующее: откройте консоль BM под учетной записью администратора домена и включите доменную группу "sns_group" в группу локальных администраторов компьютера. После этого переавторизуйтесь в ОС под учетной записью "domain1\snsadmin" с паролем "P@ssw0rd".

Далее в описании сценариев предполагается, что все виртуальные машины стенда, кроме Sniffer, включены и работают.

Сценарии использования

Сценарий №1 "Установка компонентов Secret Net Studio в сетевом варианте"

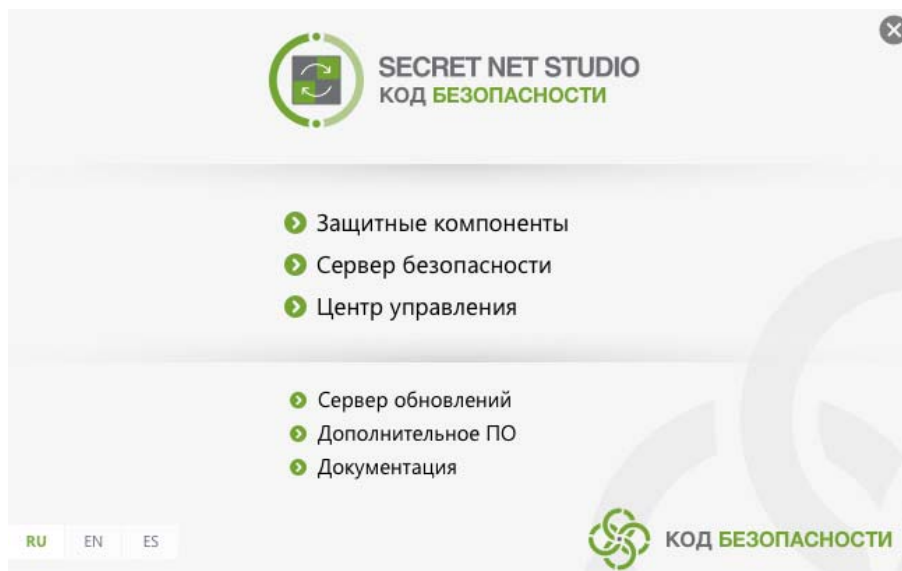
В рамках развертывания СЗИ Secret Net Studio в сетевом варианте на стенде уже выполнены соответствующие подготовительные действия на компьютерах контроллера домена и сервера безопасности.

В данном сценарии рассматривается частный случай сетевой установки SNS с формированием одного домена безопасности на базе организационного подразделения AD, которую можно разделить на следующие этапы:

- установка сервера безопасности;
- установка программы "Центр управления" (программы управления, ПУ);
- установка на защищаемые компьютеры клиента Secret Net Studio.

Сначала устанавливается сервер безопасности.

1. На BM SNS_Server под учетной записью "snsadmin" из папки "C:\Distrib\SNS_8_8_XXXXX\" дистрибутива Secret Net Studio запустите файл "SnAuto-Run.exe". Поскольку программа установки запущена в серверной ОС, будут доступны различные варианты.

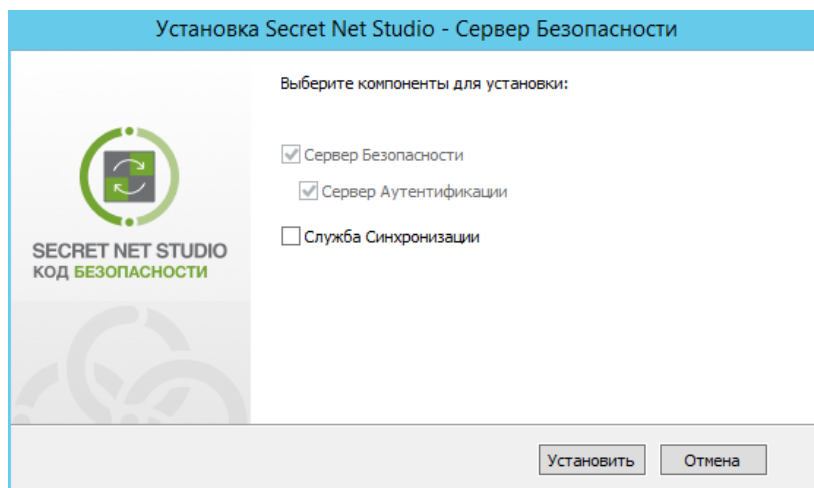


2. Выберите опцию "Сервер безопасности". Откроется окно установки Secret Net Studio. На начальном этапе выполняется анализ системы на соответствие программным и аппаратным требованиям и проверяется текущее состояние встроенного в ОС механизма управления учетными записями (UAC).

Внимание! В случае появления сообщения о необходимости отключения UAC и перезагрузки компьютера нажмите кнопку "Да", перезагрузите компьютер и снова запустите установку сервера безопасности SNS.

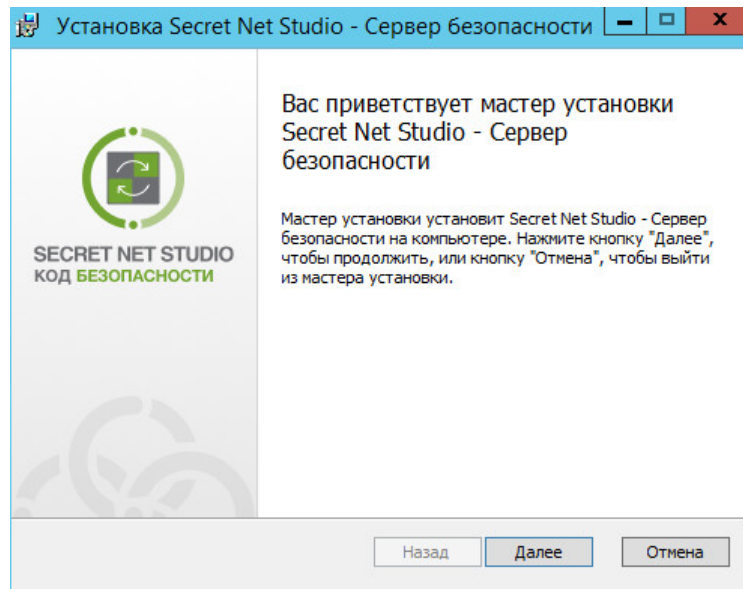
3. По окончании проверки системы на экране появится окно с перечнем устанавливаемых компонентов, позволяющее дополнительно выбрать для установки службу синхронизации.

Оставьте флажок компонента службы синхронизации пустым, поскольку в конфигурации стенда один сервер безопасности и поэтому нет необходимости обеспечивать его взаимодействие с другим сервером безопасности.

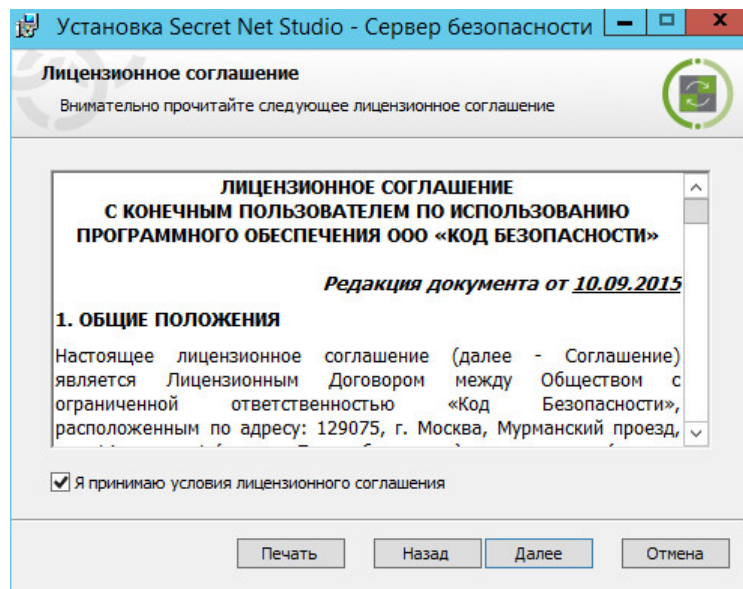


Примечание. Служба синхронизации устанавливается на сервере безопасности, чтобы, выполняя функцию шлюза, обеспечить взаимодействие этого сервера с родительским сервером безопасности. Установка данной службы выполняется отдельной программой установки, которая будет автоматически запущена после завершения установки сервера безопасности.

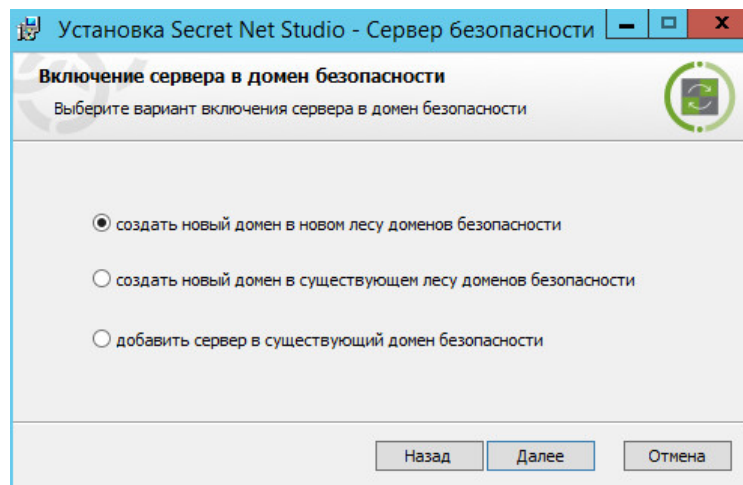
4. Нажмите кнопку "Установить". После выполнения подготовительных действий на экране появится окно приветствия мастера установки.



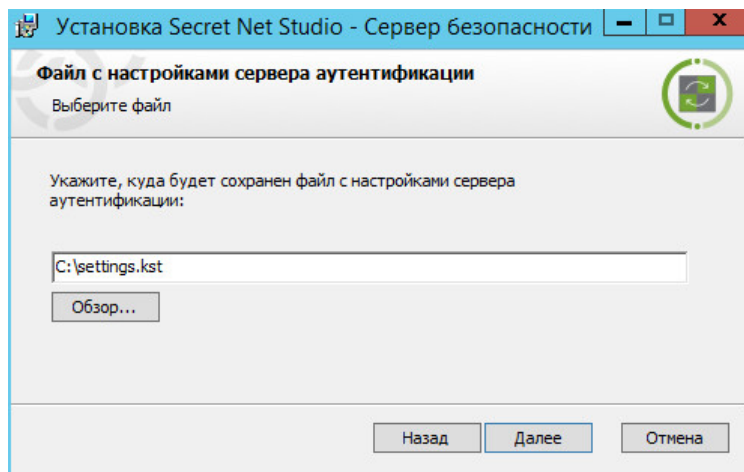
5. Нажмите кнопку "Далее". На экране появится окно принятия лицензионного соглашения. Ознакомьтесь с его содержанием и установите флажок в поле "Я принимаю условия лицензионного соглашения".



6. Нажмите кнопку "Далее". На данном шаге нужно выбрать вариант включения сервера в домен безопасности. Убедитесь, что установлен переключатель "создать новый домен в новом лесу доменов безопасности".

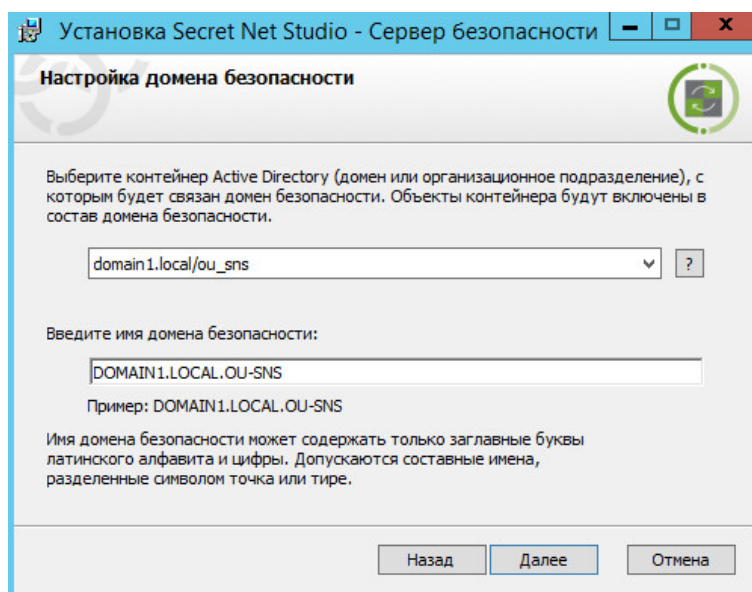


7. Нажмите кнопку "Далее". Появится окно сохранения файла с параметрами подключения сервера аутентификации в новом домене безопасности.



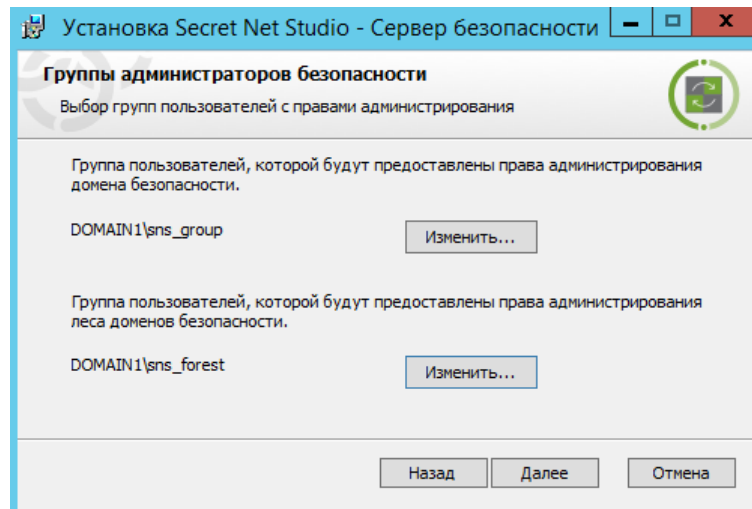
Этот файл содержит данные для развертывания новых серверов безопасности в этом домене безопасности. Поэтому для него необходимо обеспечить условия надежного хранения с защитой от компрометации содержащихся в нем данных.

8. Оставьте предлагаемое по умолчанию место сохранения файла с настройками сервера аутентификации и нажмите кнопку "Далее". В следующем окне из раскрывающегося списка нужно выбрать контейнер для формирования нового домена безопасности. В качестве него можно указать OU, в которое входит компьютер, или любое вышестоящее OU, в том числе и весь домен AD. В рамках данного документа для связи с доменом безопасности убедитесь, что выбран созданный ранее в AD контейнер "domain1.local/ou_sns", и оставьте предлагаемое по умолчанию имя создаваемого домена безопасности – **DOMAIN1.LOCAL.OU-SNS**.

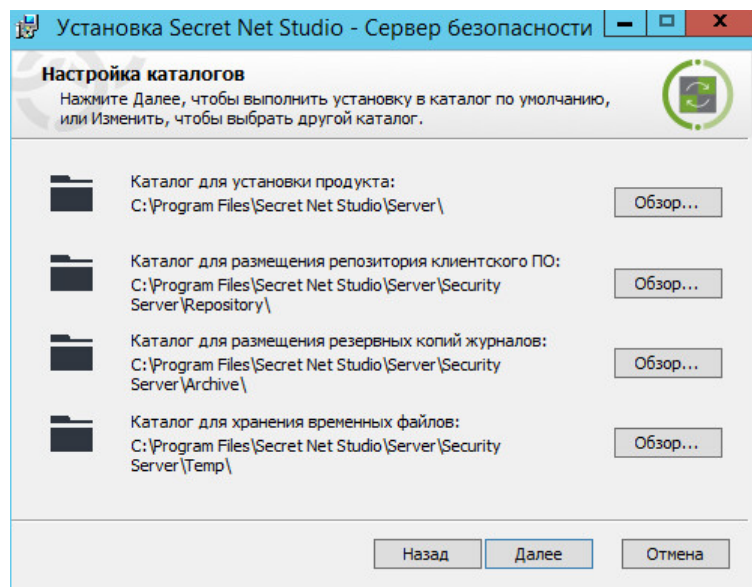


9. Нажмите кнопку "Далее". В окне выбора групп администраторов безопасности с помощью кнопок "Выбрать" укажите:
- "Группа пользователей, которой будут предоставлены права администрирования домена безопасности" – "sns_group";
 - "Группа пользователей, которой будут предоставлены права администрирования леса доменов безопасности" – "sns_forest".

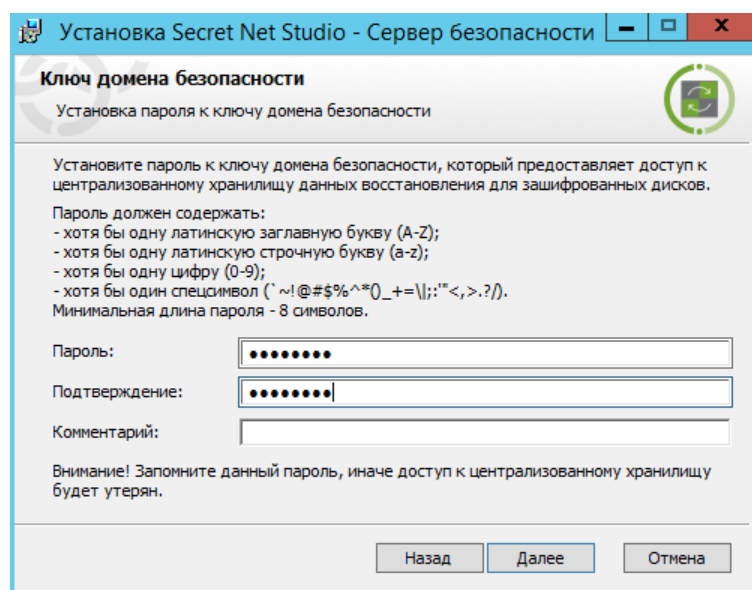
В рамках данного сценария мы будем формировать только один домен безопасности в лесу доменов безопасности.



10. Нажмите кнопку "Далее". На экране появится окно настройки каталогов. Оставьте заданные по умолчанию каталоги установки сервера безопасности и размещения служебных файлов.



11. Нажмите кнопку "Далее". Откроется окно установки пароля доступа к ключу домена безопасности. Ознакомьтесь с приведенным описанием и в полях "Пароль" и "Подтверждение" укажите **P@ssw0rd**.



Ключ и пароль предназначены для предоставления доступа к централизованному хранилищу данных восстановления для зашифрованных дисков. Пароль должен удовлетворять указанным в окне требованиям.

Внимание! В реальной работе пароль к ключу домена безопасности следует запомнить, иначе доступ к централизованному хранилищу данных восстановления будет утерян.

12. Нажмите кнопку "Далее". Откроется окно ввода информации для подключения к СУБД. Здесь нужно указать параметры соединения с тем экземпляром БД, который предназначен для работы с устанавливаемым сервером безопасности. Введите следующие значения:

- "Имя БД" – **SNS-Server\SQLEXPRESS**;

Порт можно не указывать, если используется номер по умолчанию – 1433.

- "Имя схемы БД" – оставьте вариант по умолчанию **SN7_SERVER_SCHEMA**;
- "Учетная запись администратора БД": "Имя" – **sa**, "Пароль" – **P@ssw0rd** (эта УЗ была создана при установке SQL-сервера);
- "Учетная запись, используемая сервером для доступа к БД": "Имя" – **sqluser**, "Пароль" – **P@ssw0rd**. Обратите внимание, что создается новая учетная запись, которая будет использоваться для доступа сервера безопасности к БД.



Очень часто эту учетную запись создают сами администраторы, что является распространенной ошибкой, из-за которой программа управления не подключается! Она должна создаваться только инсталлятором Secret Net Studio, а не заранее.

13. Нажмите кнопку "Далее". Откроется окно для ввода названия организации и подразделения, которое будет обслуживать устанавливаемый сервер. Введите произвольные сведения.

Эти данные будут использоваться при генерации сертификата сервера безопасности. Названия организации и подразделения могут быть введены позднее или заменены другими при выполнении процедуры "Генерация и установка сертификата сервера безопасности".

- 14.** Нажмите кнопку "Далее". В окне с сообщением о готовности к началу установки нажмите кнопку "Установить" и дождитесь окончания этого процесса.

- 15.** После завершения установки ПО СБ перезагрузите компьютер "SNS-Server" и выполните вход в систему под учетной записью "snsadmin".

Установка сервера безопасности завершена.

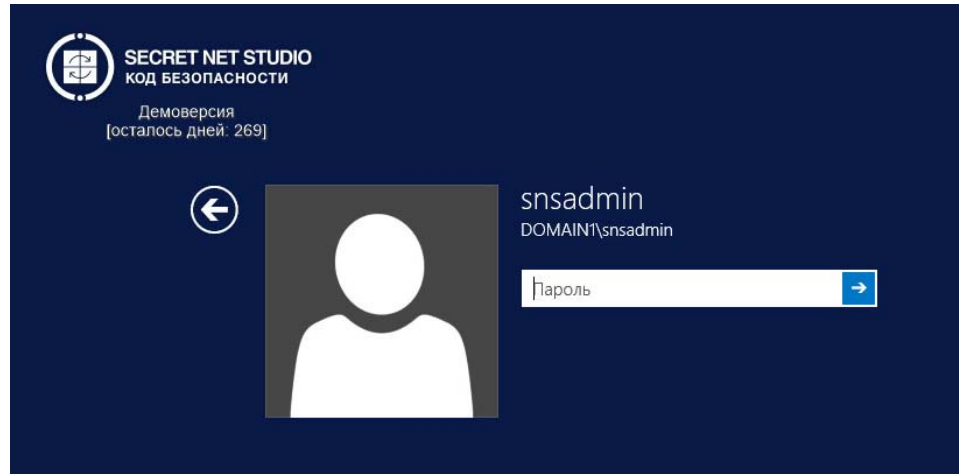
- 16.** При необходимости установки на компьютер сервера безопасности компонентов защиты SNS данную процедуру следует проводить в интерактивном режиме не централизованно. Для установки на сервер безопасности защитных компонентов выполните следующие действия:

- запустите еще раз программу установки, в открывшемся окне выберите опцию "Защитные компоненты", дождитесь завершения выполнения подготовительных действий, затем в окне лицензионного соглашения ознакомьтесь с его содержанием и нажмите кнопку "Принимаю". Появится окно выбора режима работы;

- убедитесь, что выбраны параметры для централизованного режима работы:
 - "Режим работы" – "Под управлением сервера безопасности";
 - "Сервер безопасности" – доменное имя данного сервера;
 - установлен переключатель "использовать для подключения учетную запись текущего пользователя" – поскольку авторизация в ОС выполнена с УЗ администратора домена безопасности;
- нажмите кнопку "Далее". Откроется окно выбора лицензий и формирования списка устанавливаемых защитных подсистем;

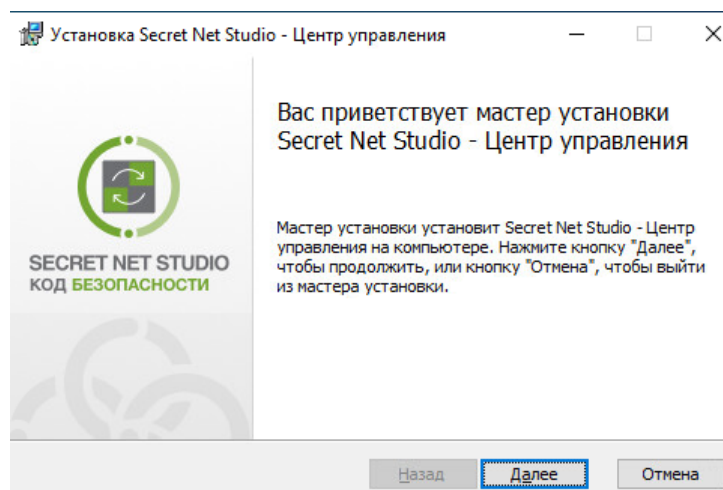
Компонент	Лицензия	Примечание
☐ Базовая защита	Обязател...	Обязательный компонент
☐ Дискреционное управление доступом	Компонен...	
☐ Затиранье данных	Компонен...	
☐ Контроль устройств	Компонен...	
☐ Замкнутая программная среда	Компонен...	
☐ Полномочное управление доступом	Компонен...	
☐ Контроль печати	Компонен...	
☐ Защита дисков и шифрование данных	Компонен...	
☐ Персональный межсетевой экран	Компонен...	
☐ Авторизация сетевых соединений	Компонен...	
☐ Полнодисковое шифрование	Компонен...	
☐ Обнаружение и предотвращение вторжений	Компонен...	
☐ Антивирус	Компонен...	
☐ Паспорт ПО	Компонен...	

- загрузите из папки "C:\Distrib" файл с полной лицензией, снимите флажок с компонента "Доверенная среда", укажите сведения о компьютере в соответствии с его наименованием в структуре тестового стенда и проведите установку защитных подсистем на сервер безопасности, после чего перезагрузите компьютер и авторизуйтесь под УЗ администратора домена безопасности "snsadmin". Обратите внимание, что на экране приветствия и авторизации MS Windows появился логотип системы Secret Net Studio.

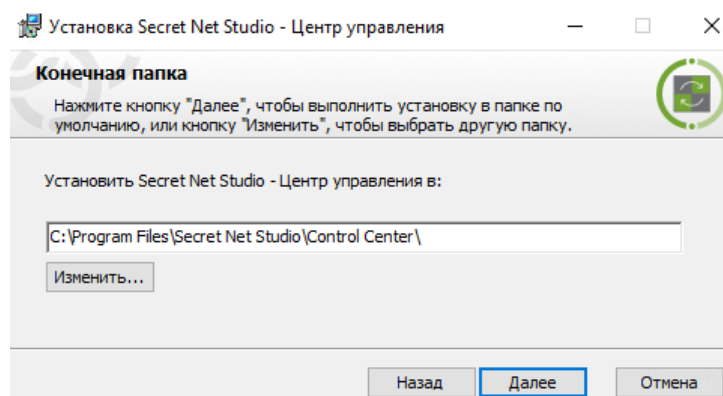


Найдите в области трея Windows значок системы Secret Net Studio , вызовите контекстное меню этого значка и откройте окно сведений о системе. Ознакомьтесь с содержащейся информацией, а затем закройте данное окно.

- 17.** Следующий этап сетевого развертывания SNS – установка на рабочем месте администратора (компьютер "Admin-VM") программы "Центр управления". Откройте консоль VM Admin_VM, авторизуйтесь под учетной записью "snsadmin", из папки "C:\Distrib\SNS_8_8_XXXXX" дистрибутива Secret Net Studio запустите файл "SnAutoRun.exe", в открывшемся окне выберите опцию "Центр управления" и дождитесь завершения подготовительных действий, в ходе которых автоматически устанавливаются или обновляются необходимые дополнительные системные компоненты.

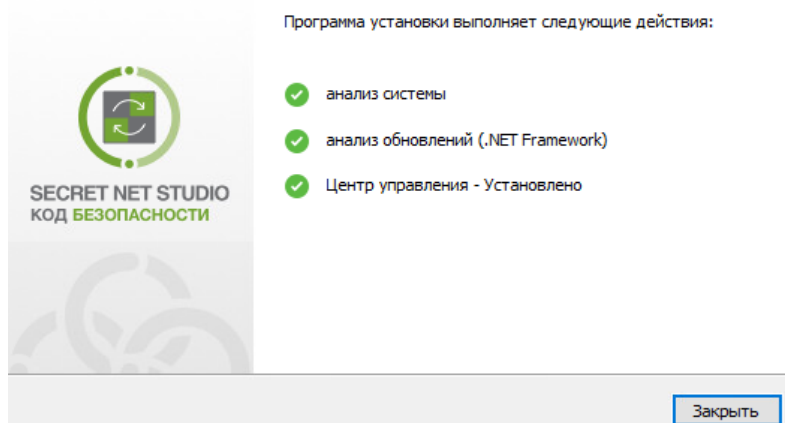


- 18.** В окне приветствия нажмите кнопку "Далее". Ознакомьтесь с текстом лицензионного соглашения, установите флажок в поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее". На экране появится окно выбора папки для установки.



19. Оставьте заданную по умолчанию папку и нажмите кнопку "Далее". В появившемся окне с сообщением о готовности к установке нажмите кнопку "Установить" и дождитесь завершения этого процесса.

Установка Secret Net Studio - Центр управления

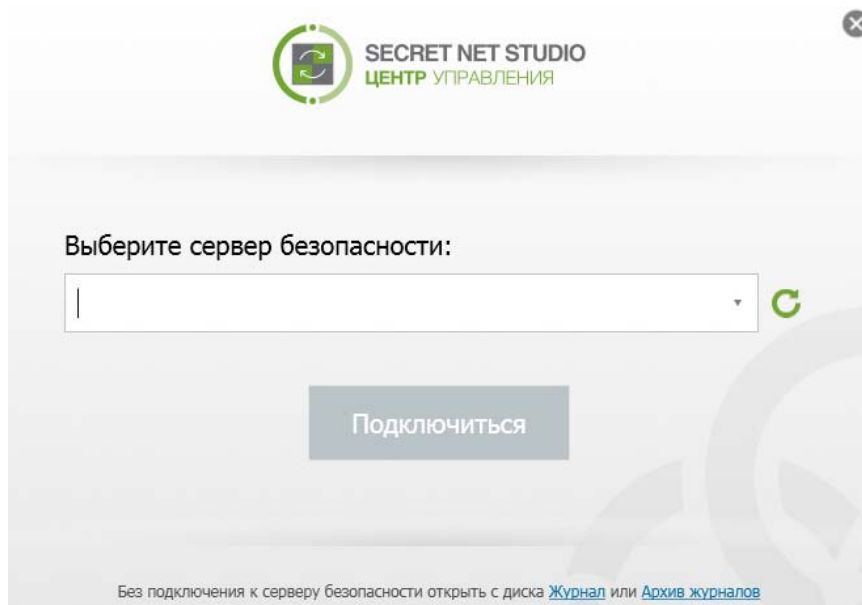


20. В окне программы установки центра управления нажмите кнопку "Заккрыть".

В стартовом окне установки SNS нажмите кнопку "Заккрыть" . Установка центра управления на рабочем месте администратора завершена.

21. Завершающий этап развертывания СЗИ Secret Net Studio в сетевом варианте – централизованная установка клиентов SNS на защищаемые компьютеры. С помощью программы управления следует подключиться к серверу безопасности и сформировать список устанавливаемого ПО и заданий развертывания. После этого на клиентских компьютерах установка ПО выполняется автоматически в фоновом режиме. При этом пользователи оповещаются о начале и завершении процесса установки, а после окончания установки выполняется перезагрузка компьютера.

Для подключения с рабочего места администратора к СБ запустите на ВМ Admin_VM программу управления: "Пуск / Код Безопасности / Центр управления" (далее – программа управления, ПУ). На экране появится стартовое окно программы.

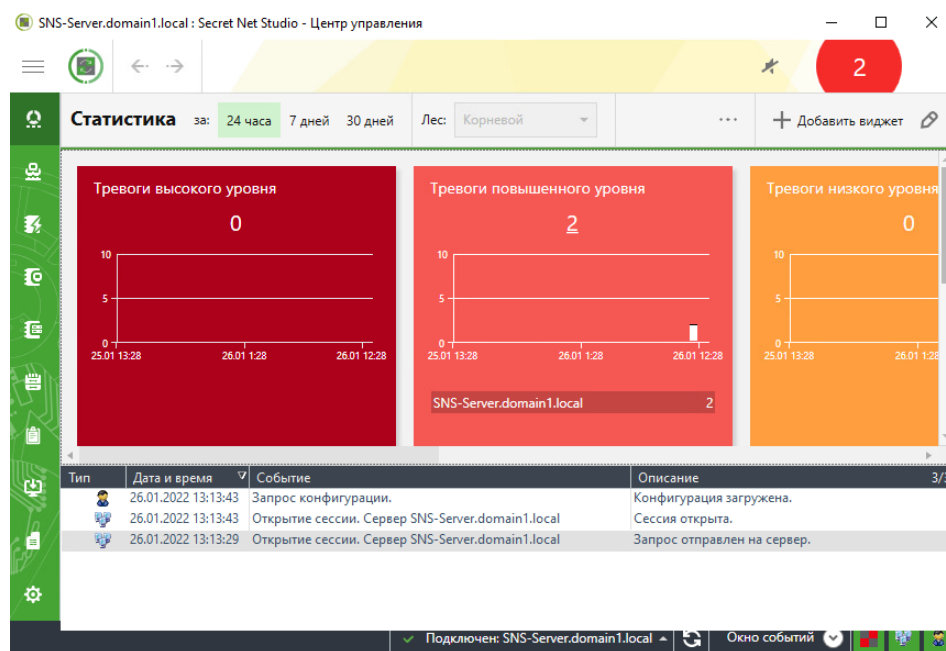


22. В поле "Сервер безопасности" введите имя сервера безопасности, с которым будет установлено соединение, – **SNS-Server.Domain1.local**, или нажмите справа от поля кнопку  для поиска зарегистрированных серверов безопасности.

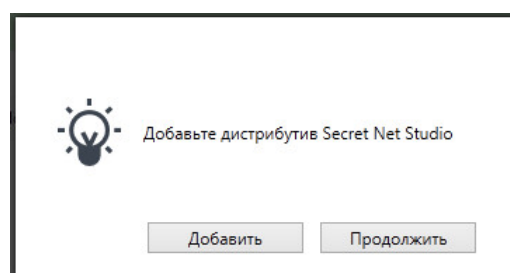
Примите к сведению. Программа предусматривает возможность запуска без подключения к серверу безопасности — для просмотра содержимого журналов, сохраненных в файлах. Для этого в нижней части стартового окна используются следующие команды:

- "Журнал" — для загрузки журнала из файла;
- "Архив журналов" — для загрузки архива журналов из файла.

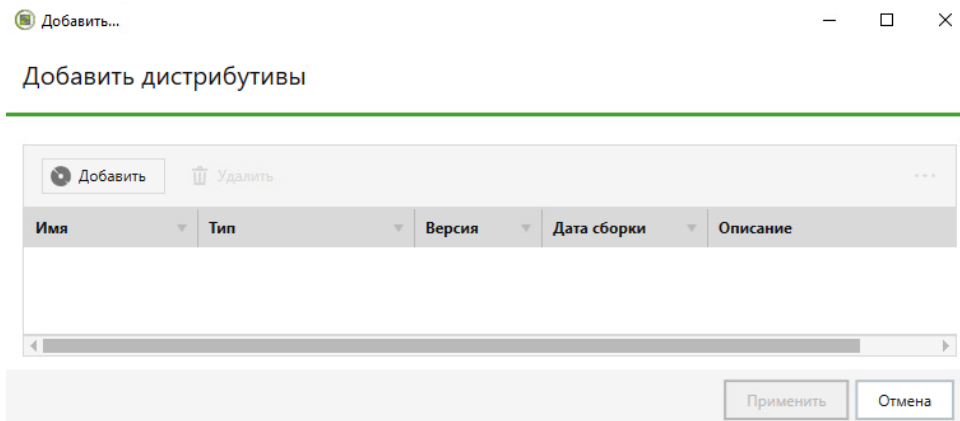
- 23.** Нажмите кнопку "Подключиться" и дождитесь завершения процедуры подключения. Обратите внимание, что в программе управления по умолчанию открылась панель "Статистика" – кнопка  в панели навигации в левой части окна выделена более темным цветовым оттенком. Эта панель содержит сведения об общем состоянии защищенности системы и состоит из виджетов – визуальных элементов интерфейса, наглядно характеризующих отдельные системные параметры.



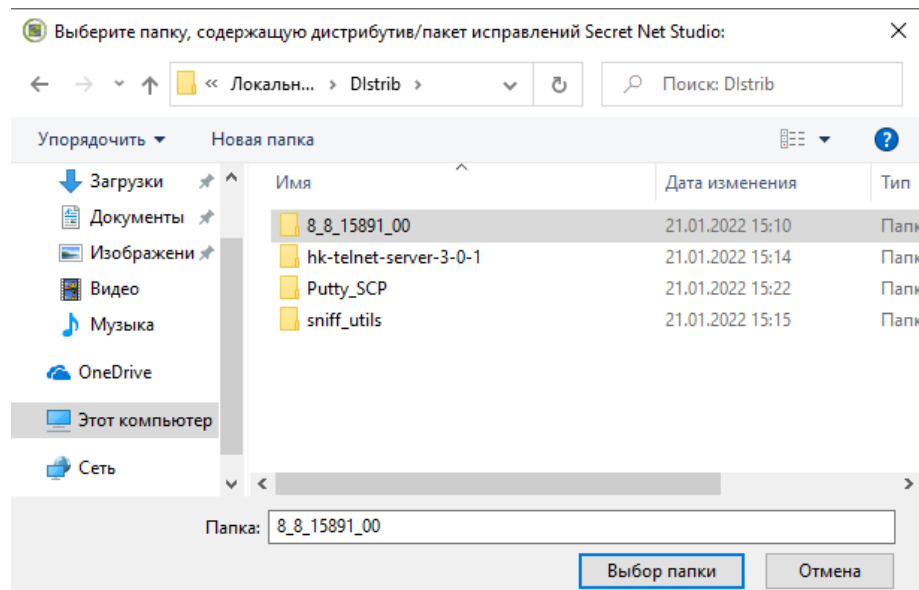
- 24.** В панели навигации нажмите кнопку "Развертывание" . В открывшемся режиме появится окно подсказки с предложением добавить в репозиторий дистрибутив Secret Net Studio. Выполните следующие действия:



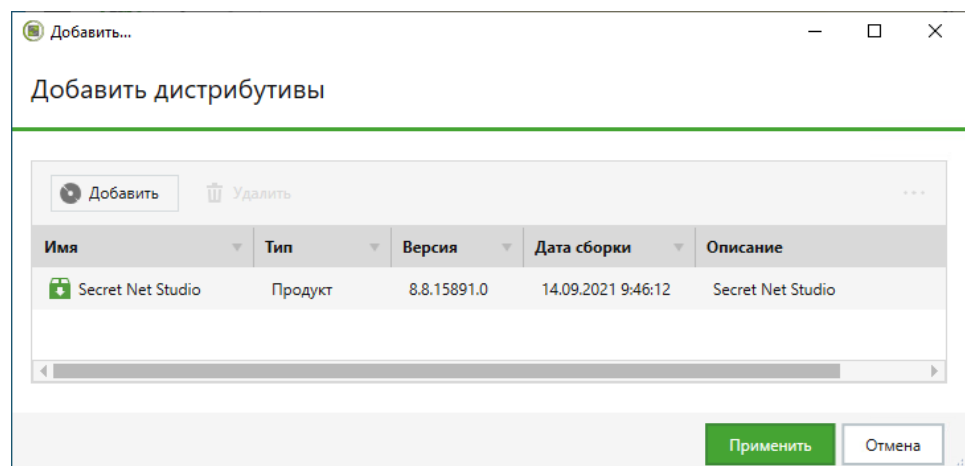
- нажмите кнопку "Добавить". На экране появится диалоговое окно для добавления комплекта установочных файлов;



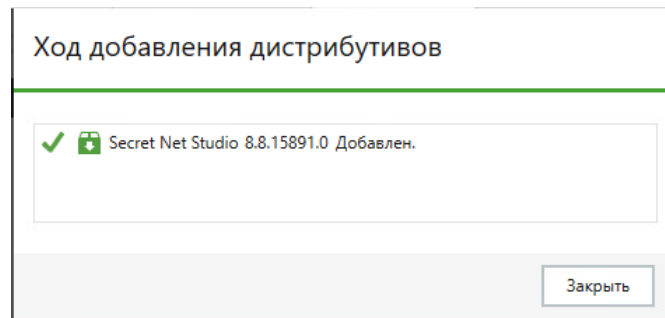
- нажмите кнопку "Добавить" и в стандартном окне выбора файлов выберите папку установки "C:\Distrib\SNS_8_8_XXXXX";



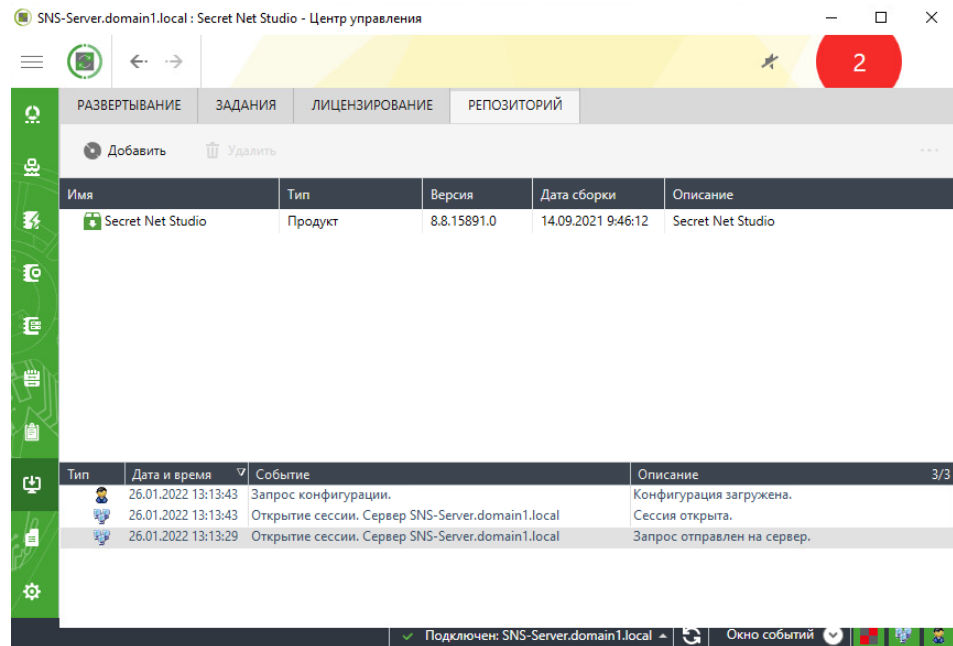
- в диалоговом окне добавления комплекта установочных файлов появится запись выбранного дистрибутива. Нажмите кнопку "Применить";



- дождитесь завершения создания установочного комплекта (процесс отправки файлов на сервер безопасности может занять продолжительное время). По окончании данного процесса нажмите кнопку "Заккрыть".



- 25.** На вкладке "Репозиторий" программы управления в списке появится новый элемент, содержащий сведения о загруженном комплекте.

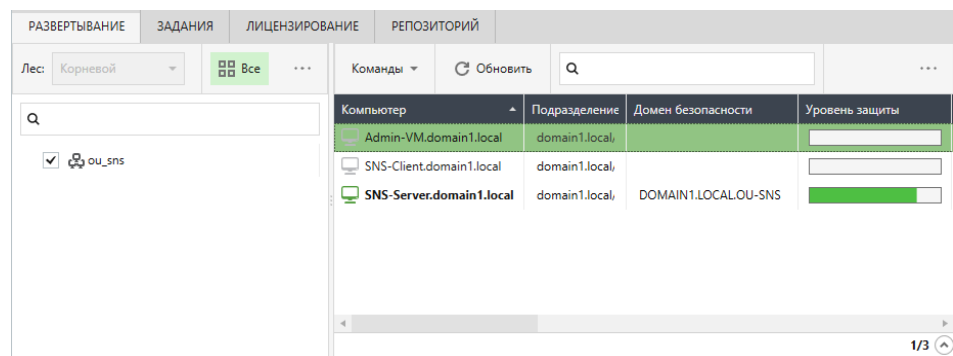


Примите к сведению. Комплекты установочных файлов помещаются на сервере безопасности в каталог "Repository", который создается при установке ПО СБ в каталоге установки сервера, и ему назначаются нужные права общего доступа. Не следует менять права доступа к данному каталогу, иначе централизованная установка ПО станет невозможна.

- 26.** После добавления комплекта устанавливаемого ПО необходимо определить список компьютеров, на которых в автоматическом режиме будут выполняться нужные действия, и сформировать задания на установку клиента SNS.

Для создания списка компьютеров выполните следующие действия:

- в панели "Развертывание" переключитесь на вкладку "Развертывание";



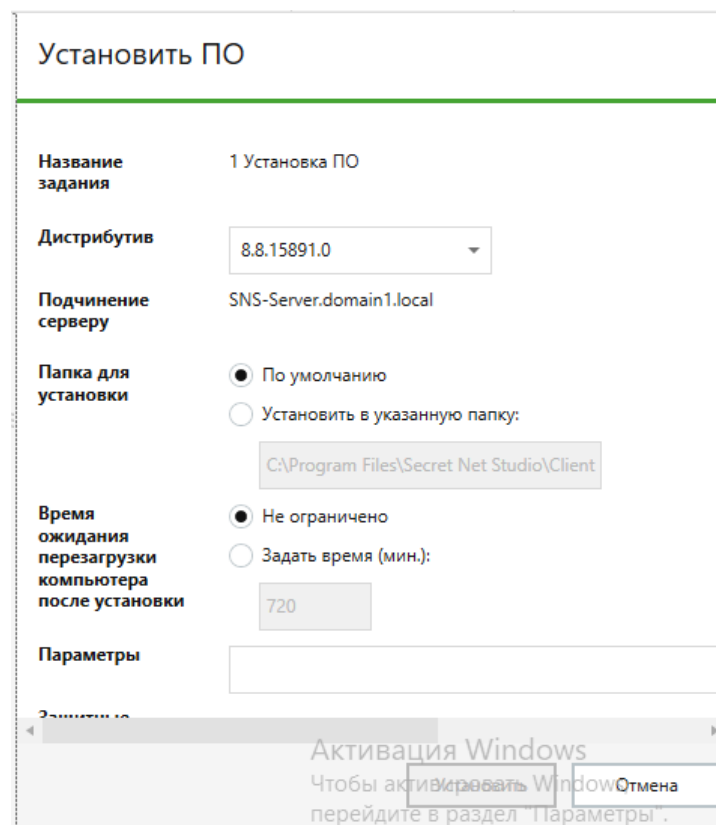
- заметьте, что список компьютеров можно фильтровать по наличию или отсутствию установленного ПО клиента (кнопки "SNS", "Без SNS" могут быть скрыты под кнопкой ) , по принадлежности контейнерам Active Directory (отображаются компьютеры тех контейнеров, которые отмечены в структуре управления слева), а также по наличию в названии заданной строки символов (поля для поиска расположены над списком контейнеров AD и над таблицей со списком компьютеров). Сортировка списка компьютеров выполняется стандартными методами с помощью заголовков колонок.

Кроме того, в таблице можно изменять состав отображаемых колонок и порядок их следования. Чтобы настроить колонки, вызовите контекстное меню в строке заголовков, выберите команду "Настройка колонок" и в появившемся диалоговом окне сформируйте список отображаемых колонок.

В текущей конфигурации тестового стенда только два компьютера, для которых нужно сформировать задание на установку компонентов SNS – это "Admin-VM" и "SNS-Client". Используя клавиши [Ctrl] или [Shift], выберите их в списке.

Примечание. Обратите внимание, что в список компьютеров для развертывания компонентов защиты не вошел контроллер домена, поскольку домен безопасности был спроецирован не на весь домен "domain1.local", а только на входящее в его состав организационное подразделение "ou_sns". Для обеспечения в организации защиты уровня 1Б следует включать в домен безопасности всю структуру AD.

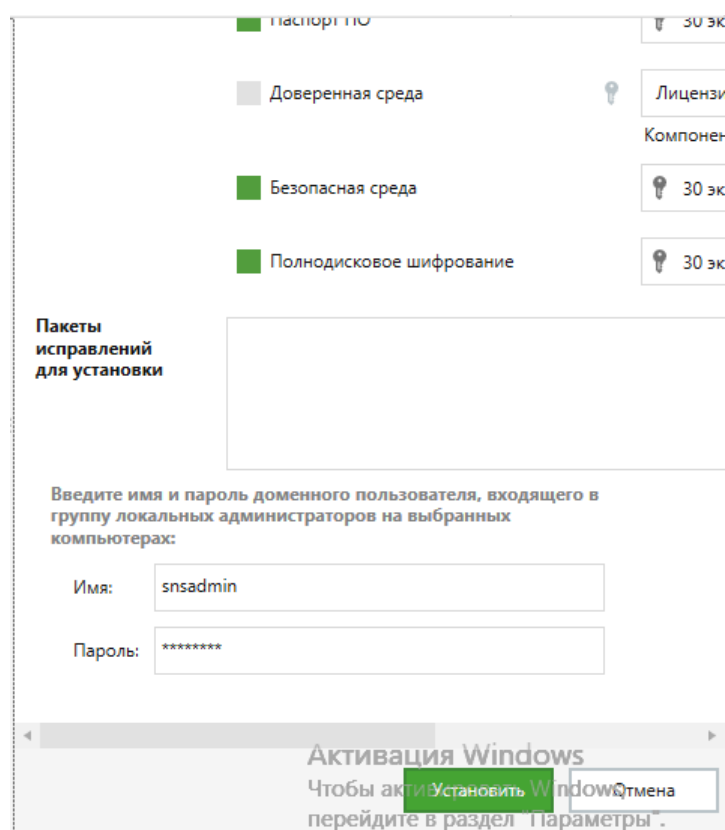
- Для формирования задания на установку ПО на выбранные компьютеры вызовите контекстное меню одного из выделенных компьютеров и выберите опцию "Установить ПО". В правой части окна появится панель настройки параметров задания.



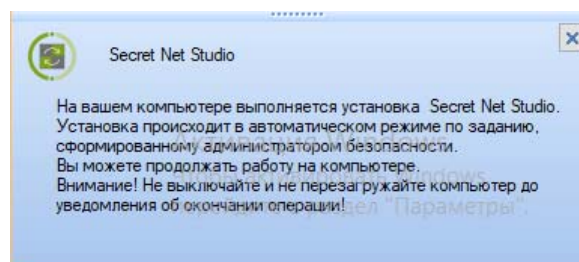
Настройте следующие параметры задания:

- "Дистрибутив" и "Папка для установки" – оставьте по умолчанию;

- "Время ожидания перезагрузки компьютера после установки" — оставьте вариант по умолчанию "Не ограничено". В этом случае автоматическая перезагрузка компьютера после установки ПО не выполняется. При необходимости включения режима автоматической перезагрузки нужно выбрать вариант "Задать время" и в поле ввода указать, через сколько минут после завершения установки следует выполнить автоматическую перезагрузку;
- "Параметры" — оставьте пустым. Данный реквизит определяет параметры командной строки, с которыми будет запущена программа установки;
- "Защитные подсистемы" – обратите внимание, что по умолчанию добавился состав лицензий из файла, который использовался при установке защитных компонентов на сервер безопасности (см. п.16). Для того чтобы добавить лицензию на компонент "Безопасная среда", нажмите кнопку "Выбрать" и выберите тот же комплект лицензий;
- поскольку компонент "Доверенная среда" может использоваться только на физическом компьютере и не активируется в виртуальной среде – снимите соответствующую отметку в списке устанавливаемых подсистем;
- учетные данные доменного пользователя, входящего в группу локальных администраторов: "Имя" – **snsadmin**, "Пароль" – **P@ssw0rd**.

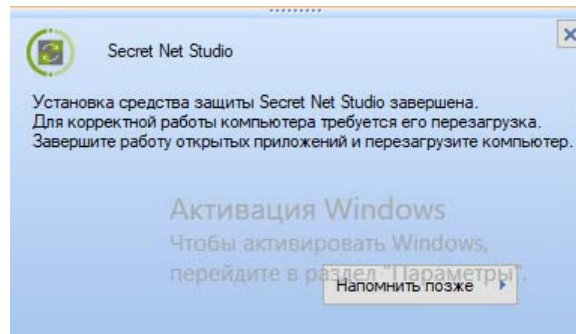


- 28.** В нижней части панели нажмите кнопку "Установить". Дождитесь окончания формирования заданий. Обратите внимание, что в окне VM Admin-VM в области уведомлений панели задач появилось уведомление о начале установки ПО.

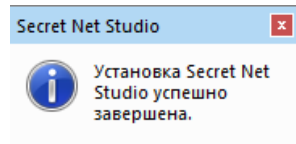


- 29.** Ознакомьтесь с текстом уведомления и закройте его. В программе управления переключитесь на вкладку "Задания". Здесь вы можете видеть состояние процесса установки выбранного ПО на указанные компьютеры списка.

До завершения процесса в области трея будет мигать значок Secret Net Studio . После завершения установки в области уведомлений окна Admin-VM появится сообщение об окончании установки.



- 30.** Последовательно переключаясь между консолями VM SNS_Client и Admin_VM, проследите за ходом установки ПО и по завершении этого процесса закройте окно уведомления и перезагрузите эти виртуальные машины. Авторизуйтесь под УЗ "snsadmin". Обратите внимание, что загрузка ОС выполняется теперь под контролем защитных механизмов SNS. В области трея Windows появился значок системы Secret Net Studio , а в области уведомлений – сообщение о завершении установки.



- 31.** Проверьте работу установленных на защищаемые компьютеры компонентов. Для этого в окне VM Admin_VM запустите "Центр управления" и подключитесь к серверу безопасности SNS-Server. В панели навигации нажмите кнопку "Компьютеры" . Откроется панель, которая содержит средства администрирования и управления компьютерами и имеет следующие режимы отображения объектов управления:

- "Диаграмма" – режим, в графическом виде показывающий сведения о структуре оперативного управления. В верхней части окна программы управления в панели инструментов слева нажмите кнопку "Диаграмма"



. Обратите внимание, что на диаграмме могут присутствовать в том числе следующие виды объектов:



– лес безопасности;



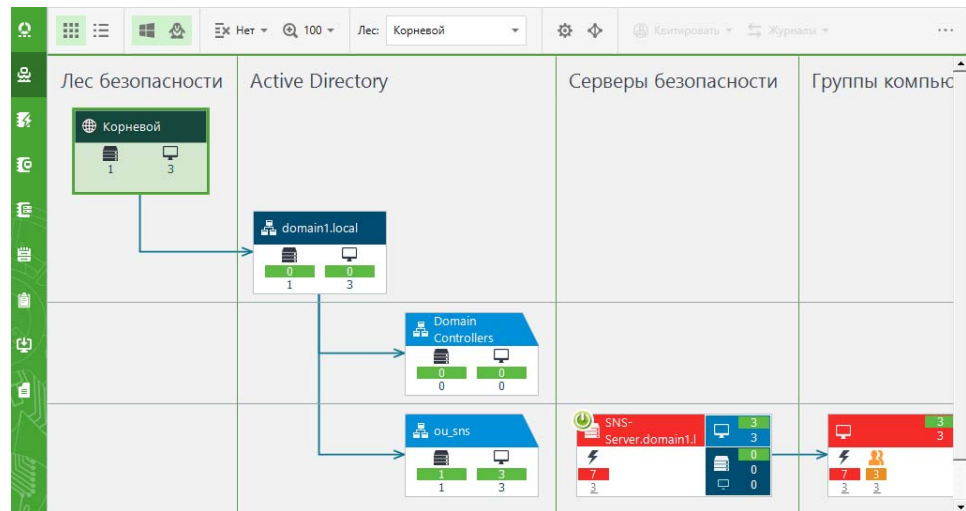
– домен или организационное подразделение;



– сервер безопасности;



– компьютер или группа компьютеров;



- "Таблица" – режим предназначен для вывода иерархического списка объектов управления в табличном виде. Нажмите кнопку "Таблица" , которая расположена слева в панели инструментов в верхней части окна программы управления. Обратите внимание, что по умолчанию защищаемые компьютеры показываются в таблице объектами структуры леса безопасности. В таблице, в частности, могут отображаться следующие значки:

Имя	Высокий	Повышенный	Низкий	ФК	Сессии	Последнее под	Лицензии	Дом
Корневой								
SNS-Server.domain1.local			1	3				DOM
SNS-Server.domain1.lo			3	3	✓	DOMAIN1\sn	Демо	DOM
SNS-Client.domain1.loc			2		✓	DOMAIN1\sn	Демо	DOM
Admin-VM.domain1.lo			2		✓	DOMAIN1\sn	Демо	DOM

 обозначает лес безопасности;

 обозначает, что объект подключен к серверу безопасности;

1 или 2 и пр. – цифры в колонках "Высокий", "Повышенный" и "Низкий" показывают количество соответствующих событий тревоги, произошедших на защищаемом компьютере и ожидающих квитирования (подтверждение приема) администратором безопасности;

значок в колонке с изображением замка обозначает, что соответствующий компьютер заблокирован;

✓ в колонке "ФК" обозначает, что пройден функциональный контроль;

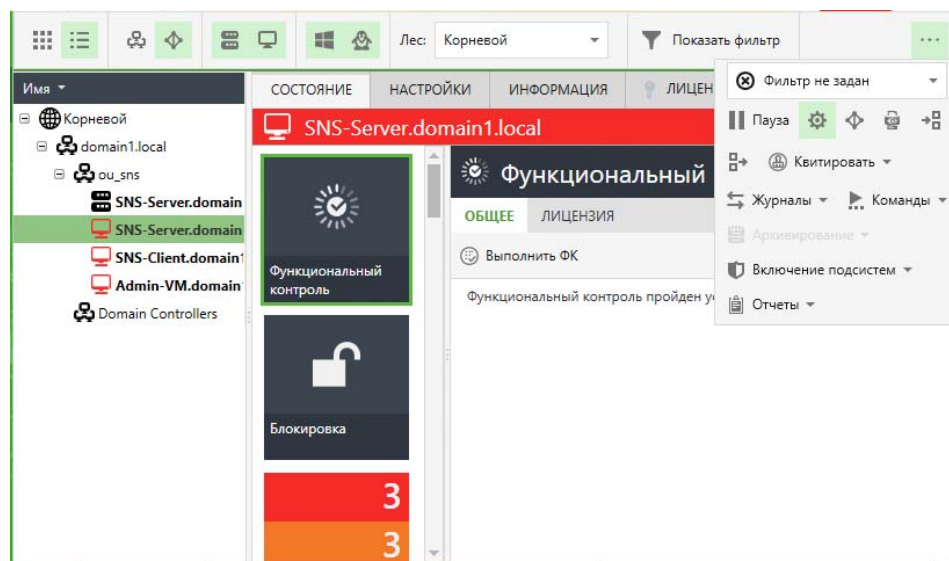
 DOMAIN1\snsadmin – значки в колонке "Сессии" показывают краткие сведения об открытых сессиях или активных пользователях. При этом цвет значка указывает на привилегированность – администратор или пользователь.

32. В панели управления нажмите кнопку "Структура AD"  Структура AD. Теперь объекты в таблице показываются в виде схемы элементов, соответствующих лесам безопасности, организационным подразделениям, серверам безопасности и защищаемым компьютерам. Схема базируется на структуре доменов и организационных подразделений в Active Directory.

33. Для того чтобы получить доступ к параметрам состояния и настройкам защиты любого объекта управляемой структуры, например, агента SNS, установленного на сервере безопасности  SNS-Server.domain1.local, выполните одну из операций:

- вызовите контекстное меню объекта и выберите опцию "Свойства";

- выделите объект и в панели управления нажмите кнопку "Свойства"  (данная кнопка может быть скрыта под кнопкой "Другие команды" , которая расположена в правой части панели управления и открывает дополнительные управляющие опции).



Примечание. В структуре оперативного управления представлены два объекта с одинаковым наименованием компьютера сервера безопасности:

 **SNS-Server.domain1.local** – указывает на агент SNS, который установлен на компьютере сервера безопасности. Этот объект используется для оперативного управления агентом, включения/отключения защитных подсистем SNS и для управления локальными политиками безопасности на данном компьютере;

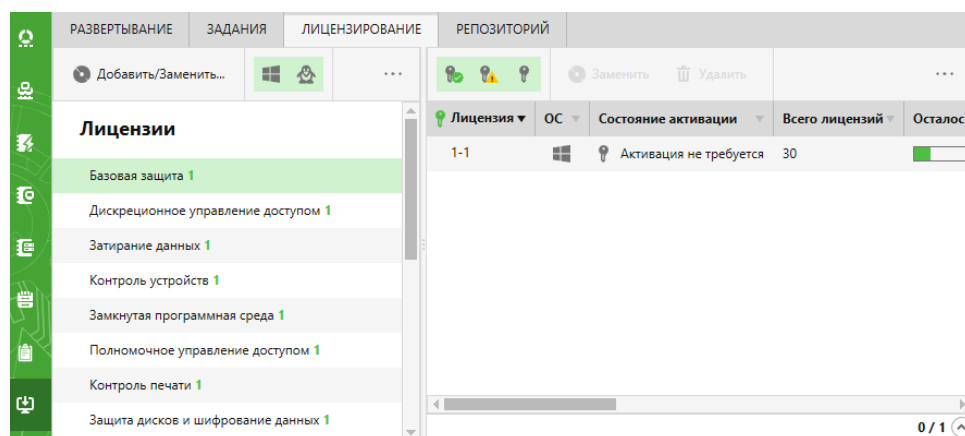
 **SNS-Server.domain1.local** – указывает на сервер безопасности SNS. Этот объект используется для управления групповыми политиками, которые будут применяться к подчиненным данному серверу компьютерам.

Далее в сценариях при указании выбрать в структуре оперативного управления элемент или объект сервера безопасности следует выделять именно сервер безопасности

 **SNS-Server.domain1.local**, а не агент SNS, установленный на компьютере СБ.

Оперативное управление (включение/отключение защитных подсистем, блокировка, перезагрузка, выключение и т.п.) выбранным объектом (агентом на защищаемом компьютере) может осуществляться через соответствующие команды его контекстного меню или кнопками панели управления.

- 34.** В панели навигации нажмите кнопку "Развертывание"  и выберите вкладку "Лицензирование", которая предназначена для просмотра и изменения сведений о зарегистрированных лицензиях на сервере безопасности.



В системе Secret Net Studio действуют лицензионные ограничения на использование ряда подсистем, реализующих применение механизмов защиты. Регистрация лицензий осуществляется с помощью специальных файлов. Лицензии можно зарегистрировать при установке защитных подсистем на сервер безопасности (см. п. 16), а также при формировании заданий развертывания ПО (см. п. 27). Кроме того, в процессе эксплуатации системы при необходимости можно зарегистрировать новые лицензии, а также заменить или удалить имеющиеся.

Закройте окно программы управления.

35. В окне консоли VM Admin_VM из главного меню Windows раскройте перечень установленных приложений и найдите группу программ "Код Безопасности". Обратите внимание, что в составе новых компонентов присутствует ПО для централизованного и локального управления:

- программа управления в централизованном ("Центр управления") и автономном ("Локальный центр управления") режимах;
- программа "Управление пользователями";
- программа "Контроль программ и данных".

Эти программные компоненты будут использоваться в других сценариях.

Сценарий №2 "Локальная настройка Secret Net Studio в соответствии с заданными параметрами"

В состав компонентов SNS, используемых для локального управления, входят следующие программные средства:

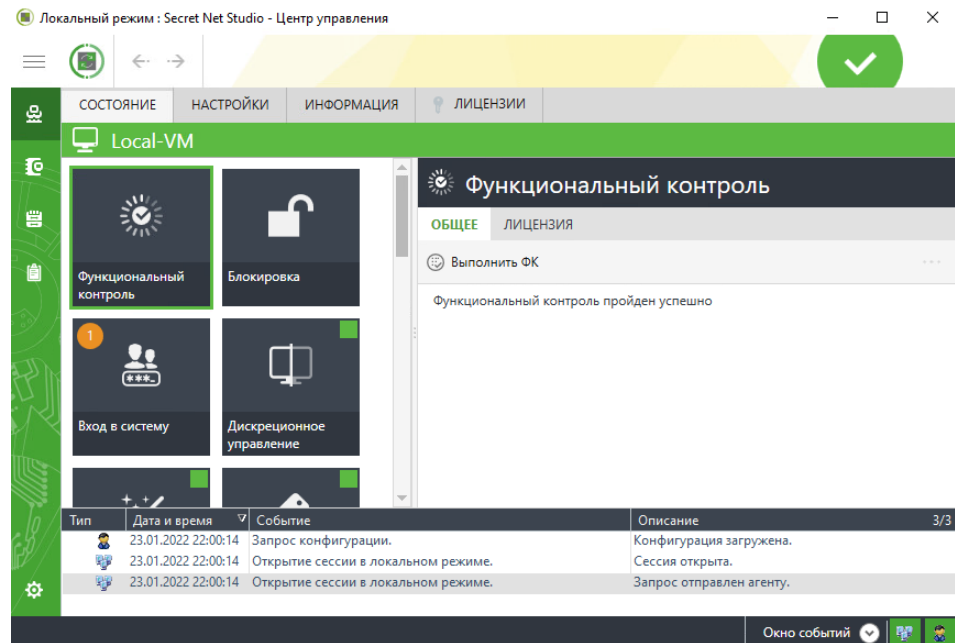
- значок Secret Net Studio в области трея Windows;
- дополнительная вкладка "Secret Net Studio" в диалоговом окне настройки свойств ресурса (файла, папки или устройства);
- программа настройки подсистемы полномочного управления доступом;
- диалоговое окно "Управление Secret Net Studio" в Панели управления Windows;
- программа "Локальный центр управления" (устанавливается в составе клиента Secret Net Studio);
- программа управления пользователями (для настройки параметров локальных пользователей);
- программа "Контроль программ и данных" в локальном режиме работы;
- дополнительные программные средства, описание работы с которыми приводится в руководстве администратора.

В данном сценарии будут рассмотрены следующие операции:

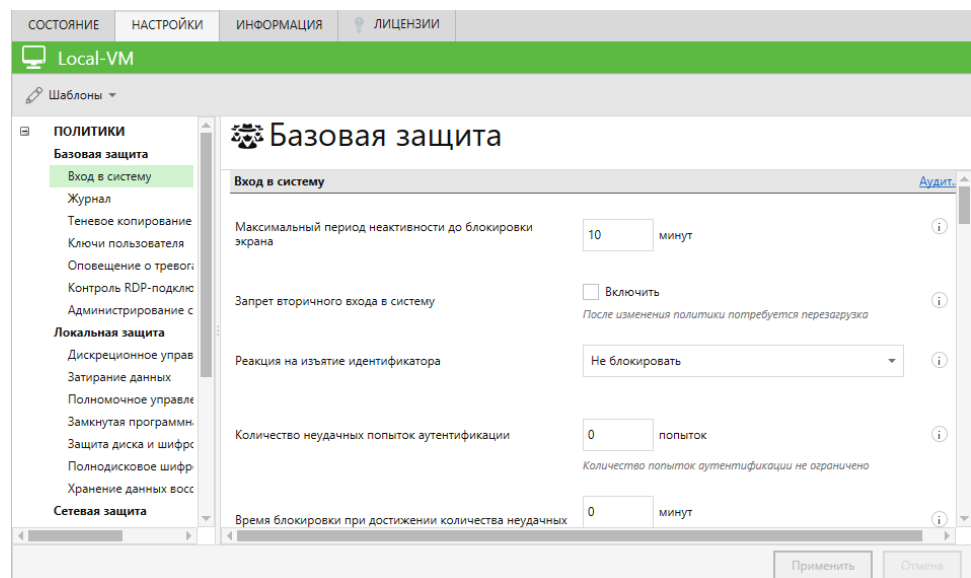
- изменение заданных по умолчанию параметров некоторых локальных политик безопасности для базовой защиты Secret Net Studio;
- изменение максимально допустимого размера журнала системы защиты Secret Net Studio и выбора регистрируемых в нем событий;
- просмотр локальных журналов в программе управления Secret Net Studio.

К локальным журналам относятся журнал Secret Net Studio и штатные журналы ОС Windows (журнал приложений, системный журнал и журнал безопасности). Программа "Локальный центр управления" позволяет просматривать хранящиеся на компьютере штатные журналы Windows и журнал SNS. Последний может просматриваться только средствами Secret Net Studio.

- 1.** Откройте консоль VM Local-VM, авторизуйтесь в ОС под учетной записью администратора "admin" и запустите программу управления в локальном режиме: "Пуск / Код Безопасности / Локальный центр управления". Откроется окно центра управления в автономном режиме.

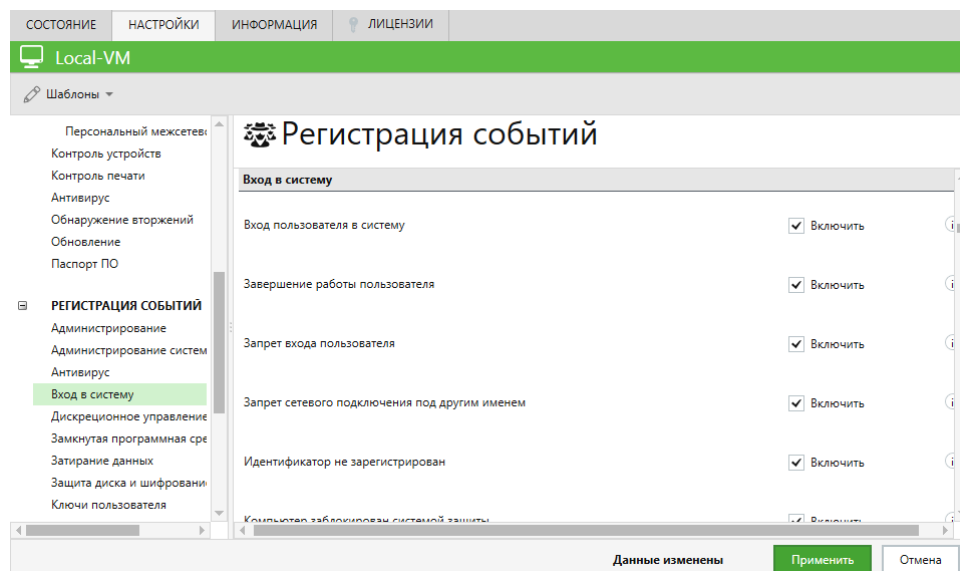


2. В панели управления "Компьютер" выберите вкладку "Настройки". В левой части окна вы увидите список настроек по разделам. В разделе "Политики / Базовая защита" выберите группу параметров "Вход в систему". В центральной части окна вы увидите текущие параметры выбранной группы.

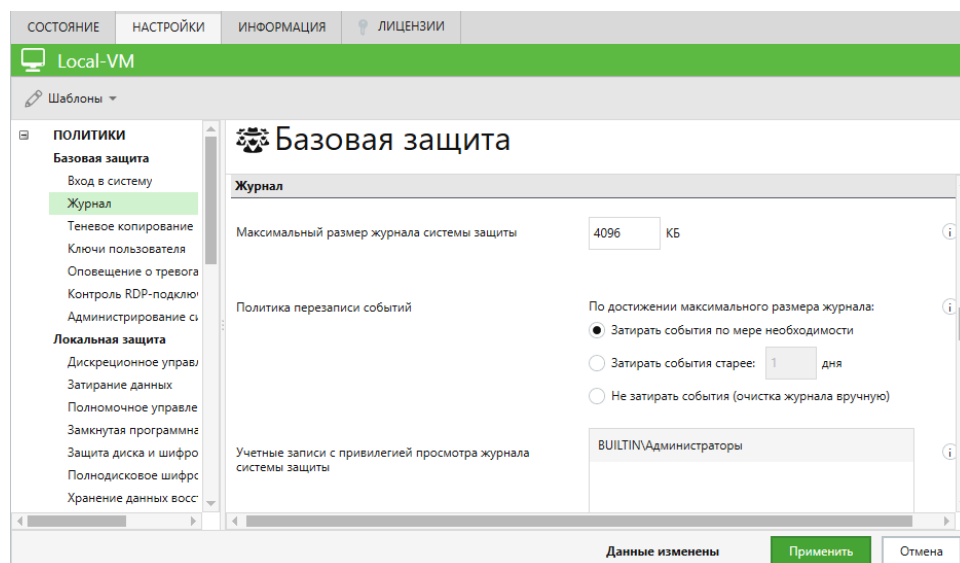


3. Обратите внимание на значок  справа от каждой настройки. Он позволяет просмотреть описание каждого параметра. Ознакомьтесь с этими описаниями.
4. Для политик группы "Вход в систему" установите следующие значения:
- "Максимальный период неактивности до блокировки экрана" – **15** минут (настройка применяется после следующего входа в систему);
 - "Запрет вторичного входа в систему" – "Включить" (обратите внимание на указание необходимости перезагрузки компьютера для применения данной настройки);
 - "Реакция на изъятие идентификатора" – оставьте значение по умолчанию "Не блокировать";
 - "Количество неудачных попыток аутентификации" – **5** (настройка применяется после следующего входа в систему);
 - "Режим идентификации пользователя" – "По имени" (настройка применяется после следующего входа в систему);

- Режим аутентификации пользователя" – оставьте вариант "Стандартная аутентификация" (изменение настройки применяется после следующего входа в систему).
5. Настройте регистрацию событий, относящихся к работе политик группы "Вход в систему". Для этого:
- в правой части заголовка группы нажмите кнопку-ссылку "Аудит". Обратите внимание, что в левой части окна теперь выбрана группа "Вход в систему" раздела "Регистрация событий", а в центральной части отображаются настройки этой группы;

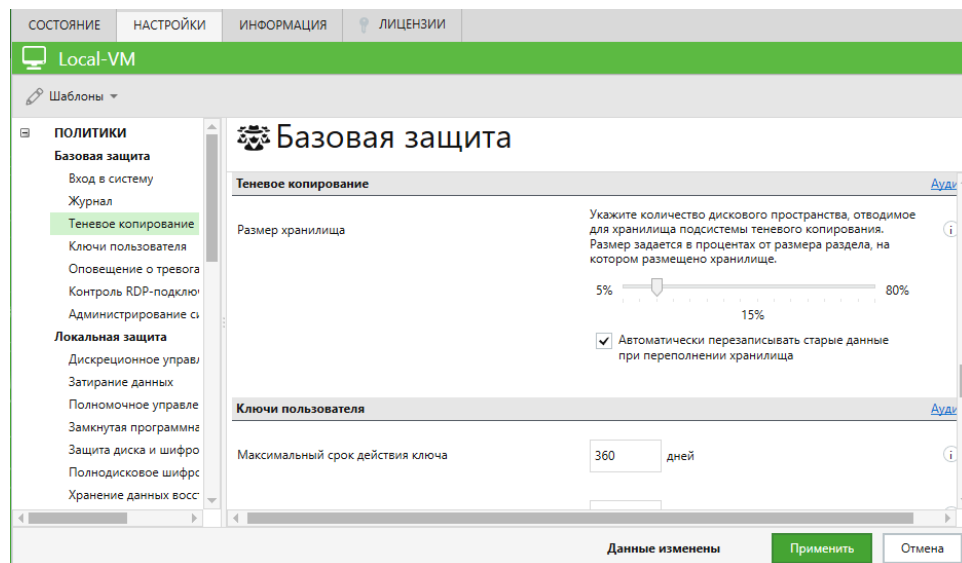


- по умолчанию включена регистрация всех событий. С помощью значка  ознакомьтесь с описаниями событий. В рамках данного сценария не выключайте регистрацию событий.
6. В левой части окна в категории "Политики / Базовая защита" выберите группу "Журнал". Установите следующие параметры:
- "Максимальный размер журнала системы защиты" – **4096** КБ;
 - "Политика перезаписи событий" – оставьте вариант "Затирать события по мере необходимости".

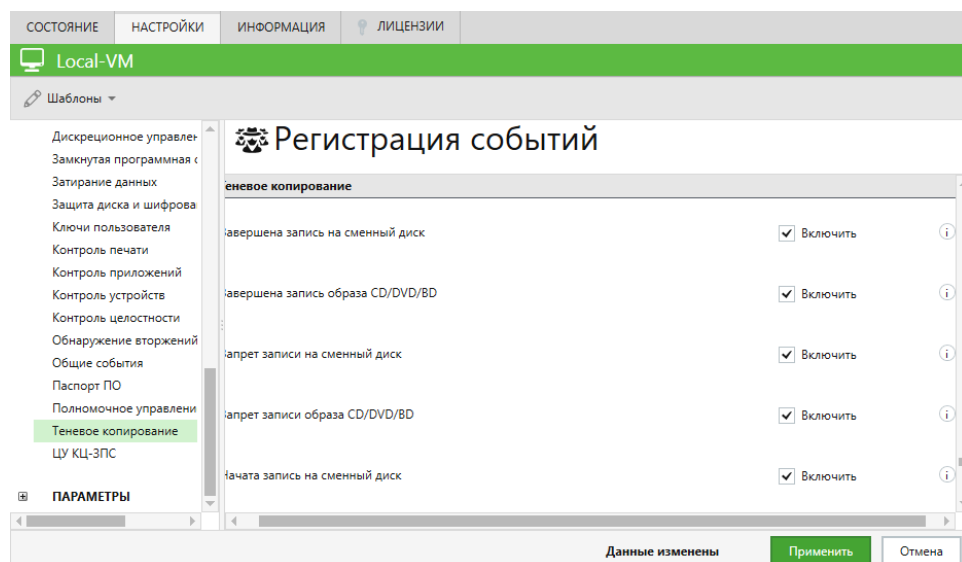


7. В категории "Политики / Базовая защита" выберите группу "Теневое копирование". Установите следующие параметры:
- "Размер хранилища" – **15%**;

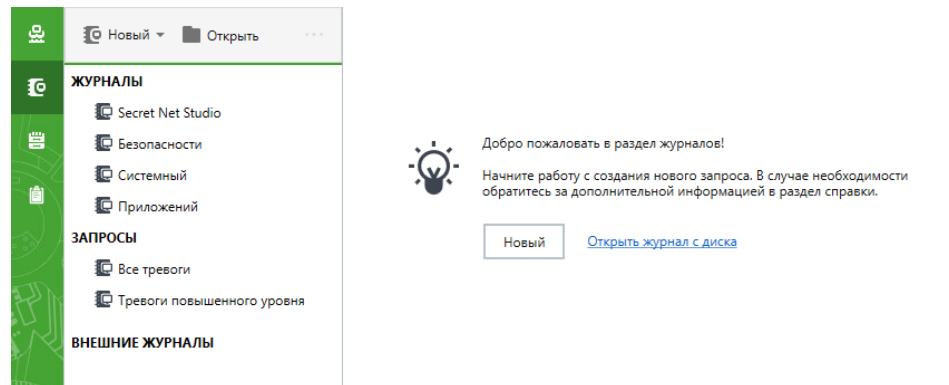
- "Автоматически перезаписывать старые данные..." – убедитесь, что в данном поле установлен флажок.



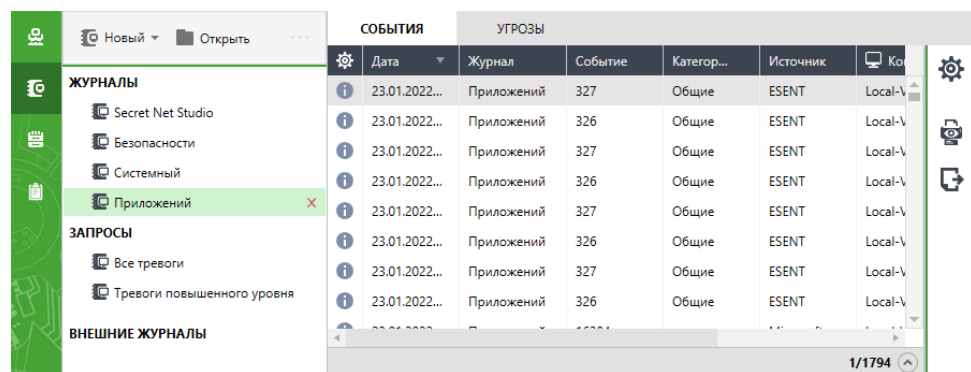
- Используя описание п. 5, просмотрите перечень типов регистрируемых событий группы "Теневое копирование".



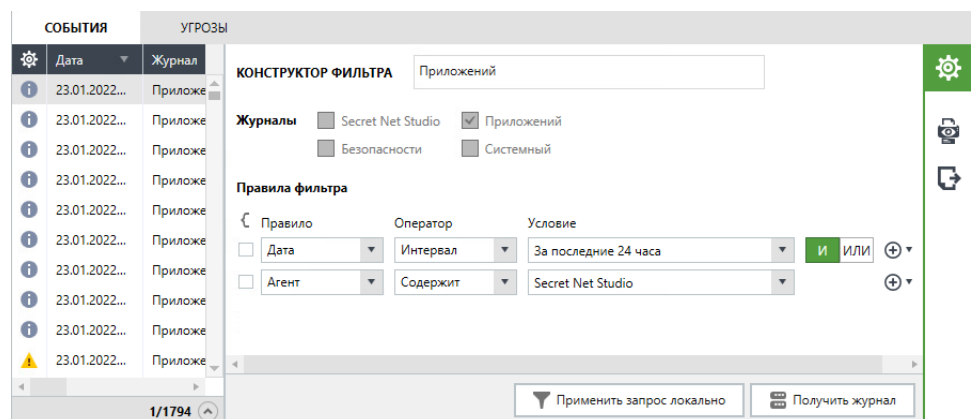
- Чтобы активировать новые установленные значения параметров политик безопасности на вкладке "Настройки", нажмите кнопку "Применить". Дождитесь завершения операции сохранения изменений и обратите внимание на появившуюся запись об изменении политик в панели событий. Перезагрузите VM Local-VM и вновь запустите программу управления.
- Просмотрите содержимое локальных журналов в программе управления Secret Net Studio. Для этого:
 - в окне программы управления Secret Net Studio в панели навигации выберите "Журналы". Вы увидите перечень доступных для просмотра локальных журналов;



- для того чтобы просмотреть полное содержимое любого из журналов, достаточно выбрать его двойным щелчком мыши. Выберите журнал приложений. Обратите внимание, что открылась вкладка просмотра записей и в правой части окна появились кнопки, позволяющие распечатать или сохранить журнал в файл на диске;



- в случае необходимости получить более конкретную выборку записей журнала можно составить запрос на формирование выборки по определенным условиям. Нажмите в правой части окна кнопку "Запрос"  и в раскрывшейся панели с помощью кнопки "Добавить правило" добавьте следующие правила: "Дата" – "Интервал" – "За последние 24 часа" и "Агент" – "Содержит" – "Secret Net Studio";



- нажмите кнопку "Применить запрос локально", закройте панель настройки запроса, нажав в правой части окна кнопку "Запрос" , и просмотрите полученный результат;
- подсистема запросов позволяет формировать выборки по более развернутым условиям, включая записи из любых локальных журналов. В панели инструментов нажмите кнопку "Новый" , установите произвольные правила фильтра, нажмите кнопку "Получить журнал" и просмотрите результат;

- последовательно просмотрите журналы безопасности и Secret Net Studio.

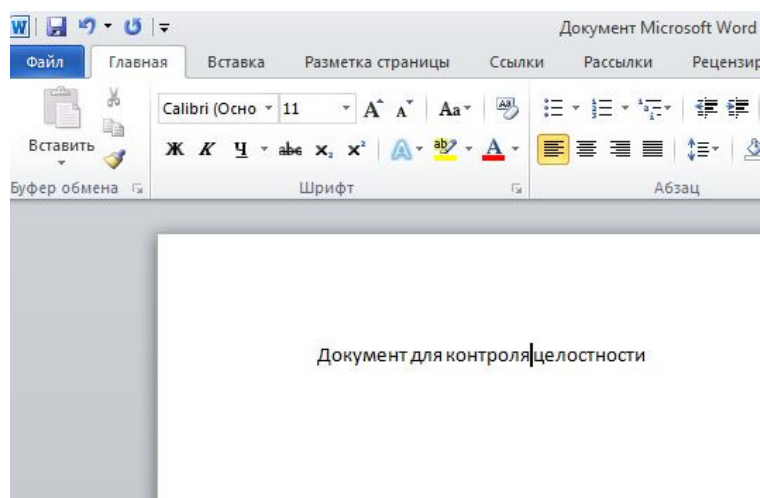
11. Изменены некоторые локальные политики, установлен максимальный размер журнала системы защиты Secret Net Studio, показана возможность выбора регистрируемых в нем событий и в программе управления SNS проведен просмотр локальных журналов.

Останьтесь в текущем окне BM Local-VM. Выполнение сценария завершено.

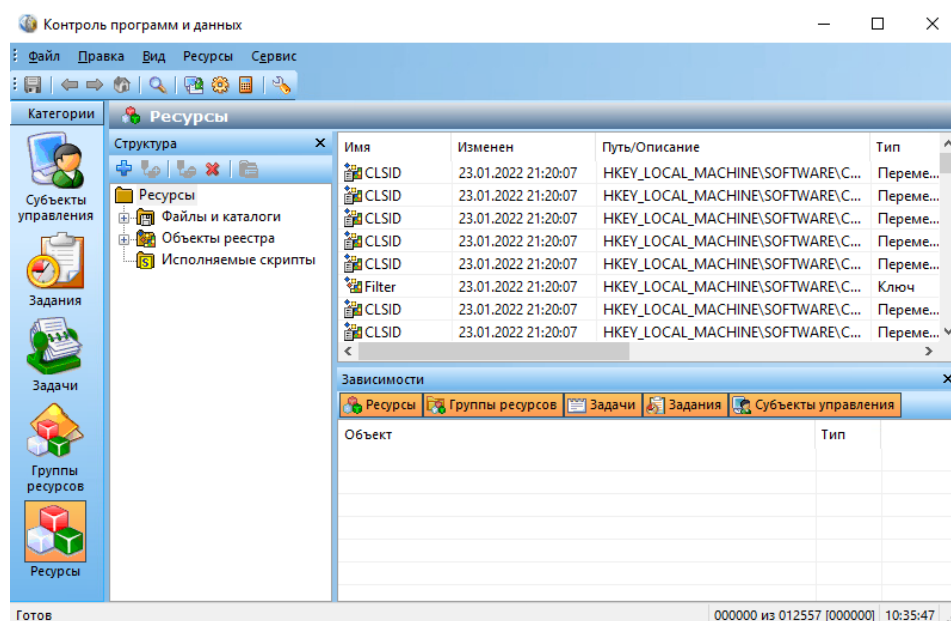
Сценарий №3 "Настройка механизма контроля целостности"

В данном сценарии показывается начальная настройка этого механизма и проверяется его работа на примере контроля целостности текстового файла формата Microsoft Word.

1. В окне BM Local-VM на диске "C:\\" создайте папку "Контроль целостности". В этой папке создайте файл "Документ Microsoft Word.docx" с произвольным содержанием, который будет контролируемым ресурсом в МД КЦ.

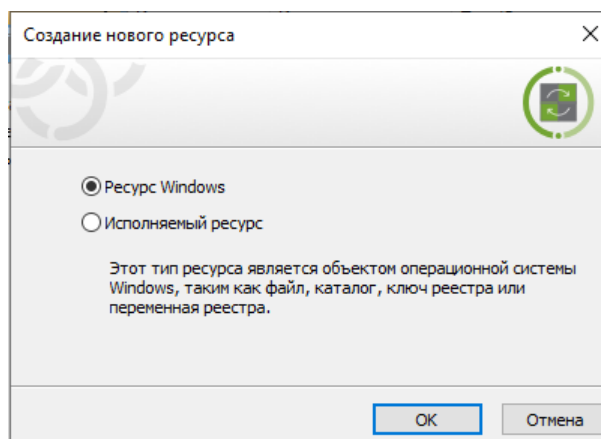


2. Запустите программу "Контроль программ и данных" в локальном режиме: "Пуск / Код Безопасности / Контроль программ и данных" и в открывшемся окне выберите категорию "Ресурсы".

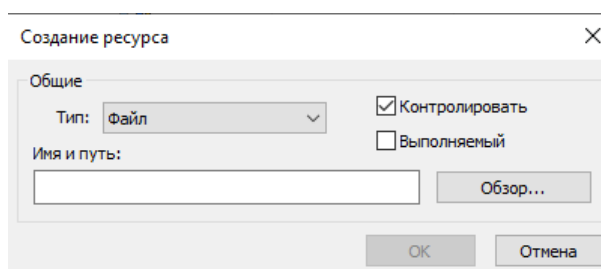


3. Подготовьте описание контролируемого ресурса (созданного ранее файла) в модели данных КЦ. Для этого:

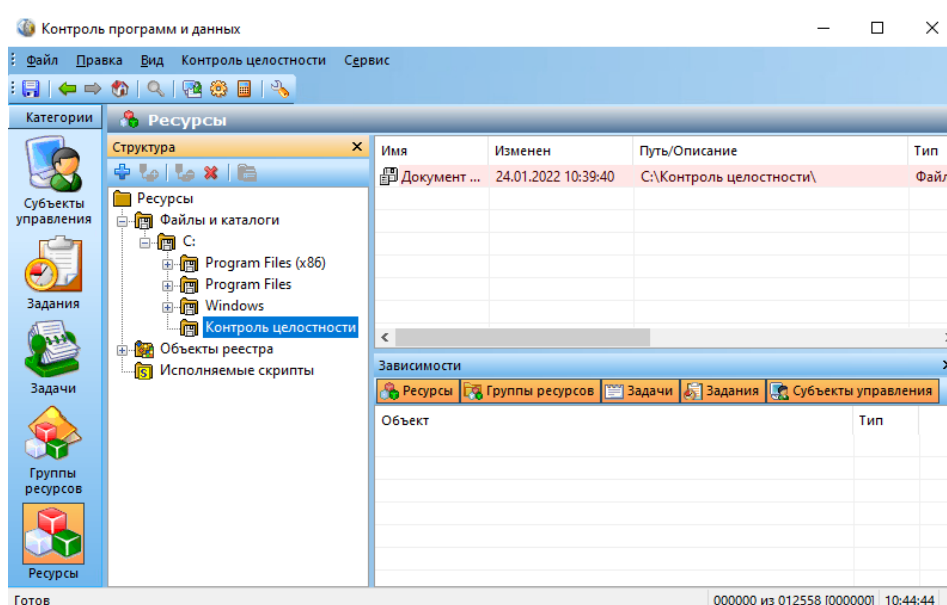
- в панели "Структура" вызовите контекстное меню папки "Ресурсы" и выберите опцию "Создать ресурс(ы) / Одиночный";



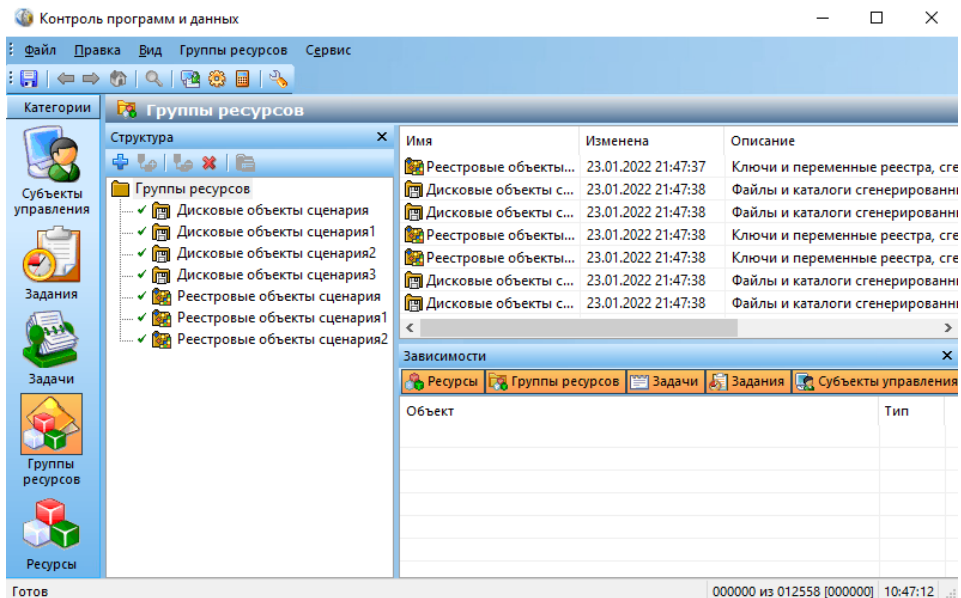
- в окне создания нового ресурса выберите тип "Ресурс Windows" и нажмите кнопку "ОК" – откроется следующее диалоговое окно создания ресурса;



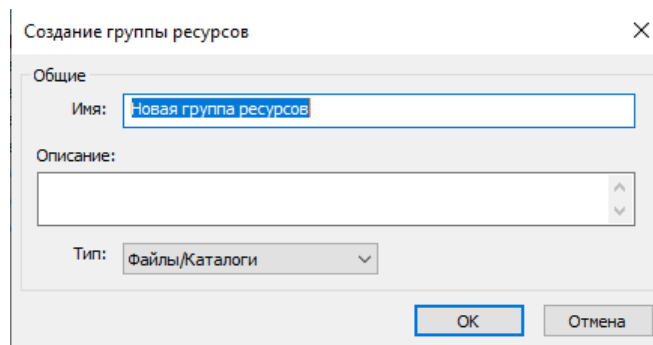
- в поле "Тип" оставьте установленный по умолчанию тип ресурса "Файл", через кнопку "Обзор" укажите путь к созданному в п. 1 файлу "Документ Microsoft Word.docx" и нажмите кнопку "ОК". Описание ресурса готово, и вы вернулись в окно "Контроль программ и данных".
4. В окне "Контроль программ и данных" в панели "Структура" разверните ветку "Ресурсы / Файлы и каталоги / C: / Контроль целостности" и найдите запись с описанием выбранного вами файла для контроля.



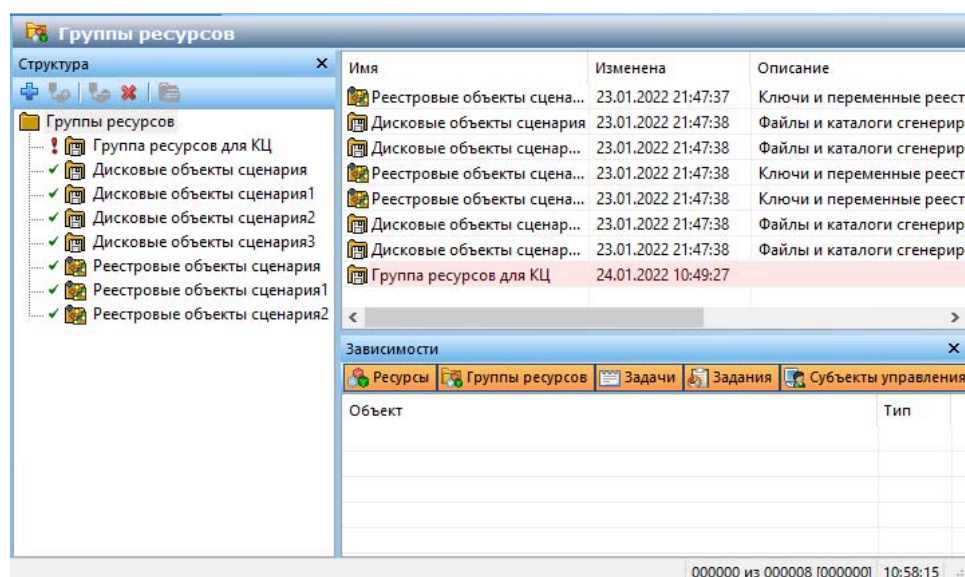
5. Согласно описанию МД КЦ, сформируйте группу ресурсов и добавьте в нее подготовленный ресурс. Для этого:
- в окне "Контроль программ и данных" выберите категорию "Группы ресурсов";



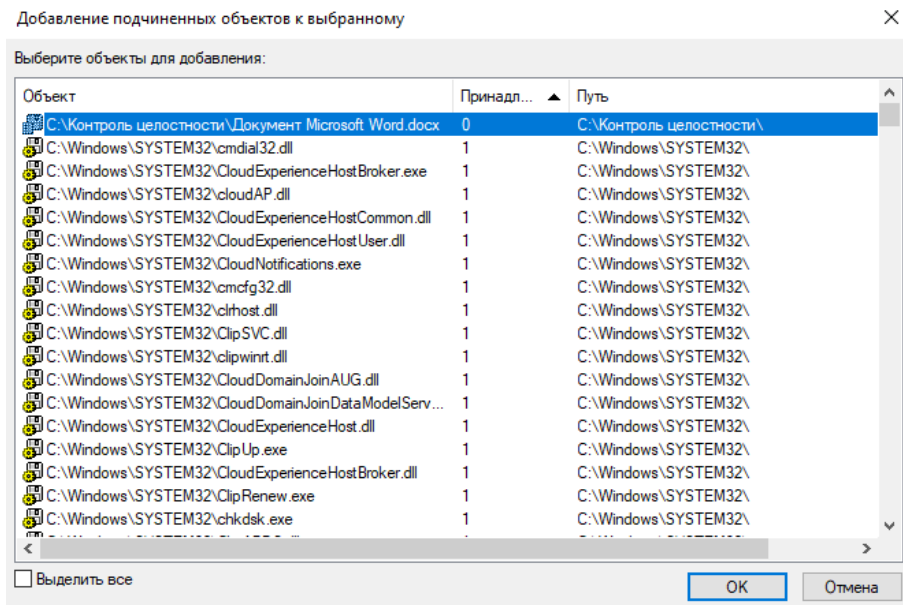
- в панели "Структура" вызовите контекстное меню папки "Группы ресурсов" и выберите опцию "Создать группу / Вручную" – откроется диалоговое окно;



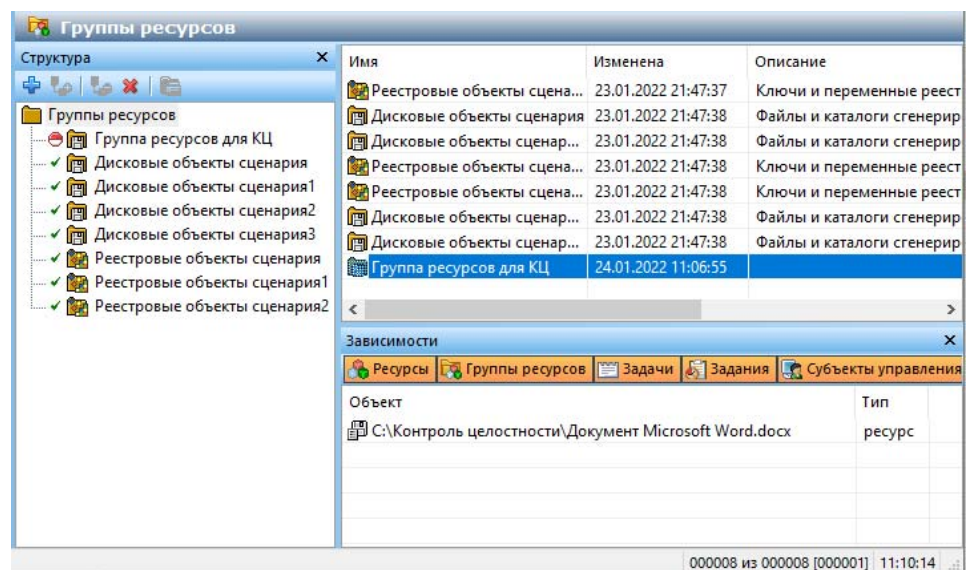
- в окне "Создание группы ресурсов" заполните поля: "Имя" – введите "Группа ресурсов для КЦ", "Описание" – произвольно. Нажмите кнопку "OK". В окне "Контроль программ и данных" появится запись с названием созданной группы. Обратите внимание, что эта группа пока пустая;



- в группу "Группа ресурсов для КЦ" добавьте созданный ранее ресурс. Для этого на записи группы щелкните правой кнопкой мыши и выберите опцию "Добавить ресурсы / Существующие";

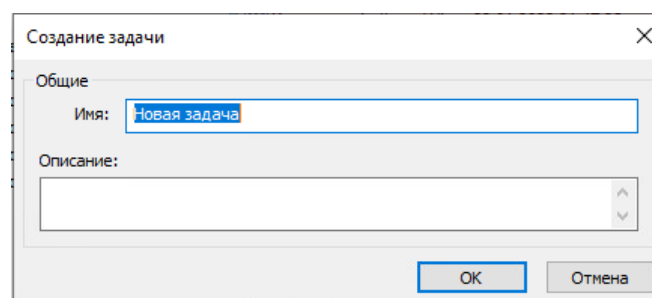


- в открывшемся диалоговом окне выделите запись подготовленного вами ранее файла ресурса "C:\Контроль целостности\Документ Microsoft Word.docx" и нажмите кнопку "OK" – в созданную группу добавлен файл ресурса.



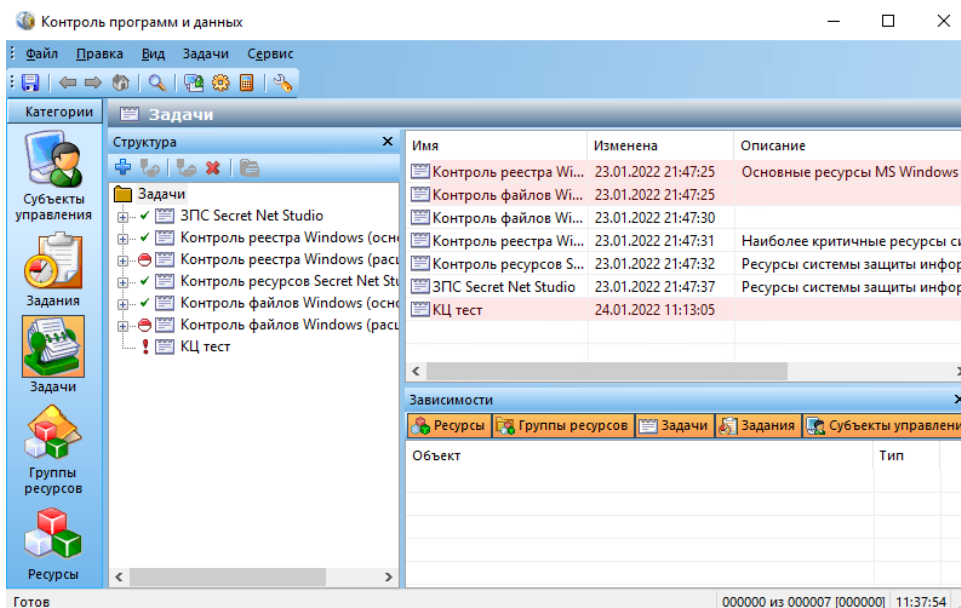
- В окне "Контроль программ и данных" создайте новую задачу и добавьте в нее подготовленную для контроля группу ресурсов. Для этого:

- выберите категорию "Задачи", вызовите контекстное меню папки "Задачи" и выберите опцию "Создать задачу / Вручную". Откроется диалоговое окно;

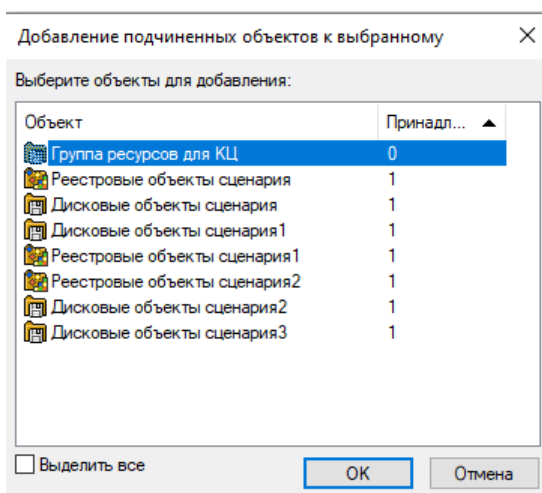


- введите в поле "Имя" – имя задачи "КЦ тест", в поле "Описание" – произвольный текст;

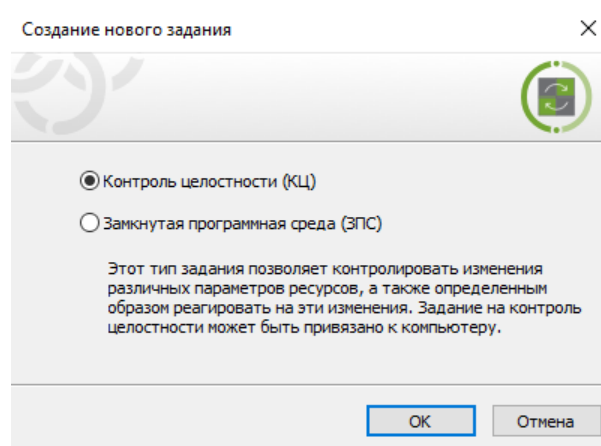
- нажмите кнопку "ОК". В структуре "Задачи" окна "Контроль программ и данных" появилась новая запись;



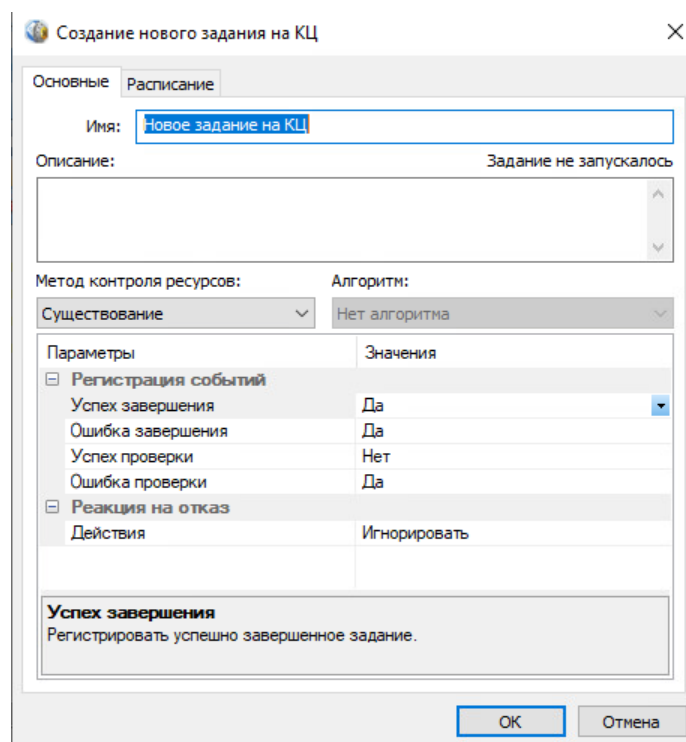
- в созданную задачу добавьте группу ресурсов для КЦ. Для этого вызовите контекстное меню задачи "КЦ тест" и выберите опцию "Добавить группы / Существующие". Откроется диалоговое окно;



- в окне "Добавление подчиненных объектов к выбранному" выберите запись "Группа ресурсов для КЦ" и нажмите кнопку "ОК" – задача создана и в нее добавлена группа.
7. В окне "Контроль программ и данных" создайте новое задание. Для этого:
- откройте категорию "Задания" и в контекстном меню папки "Задания" выберите опцию "Создать задание". Откроется диалоговое окно;



- убедитесь, что по умолчанию выбрана опция "Контроль целостности (КЦ)" и нажмите кнопку "ОК". Откроется диалоговое окно "Создание нового задания на КЦ";



- в открывшемся окне установите следующие параметры: "Метод контроля ресурсов" – "Содержимое", "Алгоритм" – "Полное совпадение", в группе параметров "Реакция на отказ" для параметра "Действие" выберите "Восстановить с блокировкой" (значение контролируемого параметра ресурса восстанавливается из эталона. Компьютер блокируется, и снять блокировку сможет только администратор безопасности);

Создание нового задания на КЦ

Основные Расписание

Имя: Новое задание на КЦ

Описание: Задание не запускалось

Метод контроля ресурсов: Алгоритм:

Содержимое Полное совпадение

Параметры	Значения
☐ Регистрация событий	
Успех завершения	Да
Ошибка завершения	Да
Успех проверки	Нет
Ошибка проверки	Да
☐ Реакция на отказ	
Действия	Восстановить с блокировкой

Действия
Действия в случае обнаружения ошибки при выполнении задания.

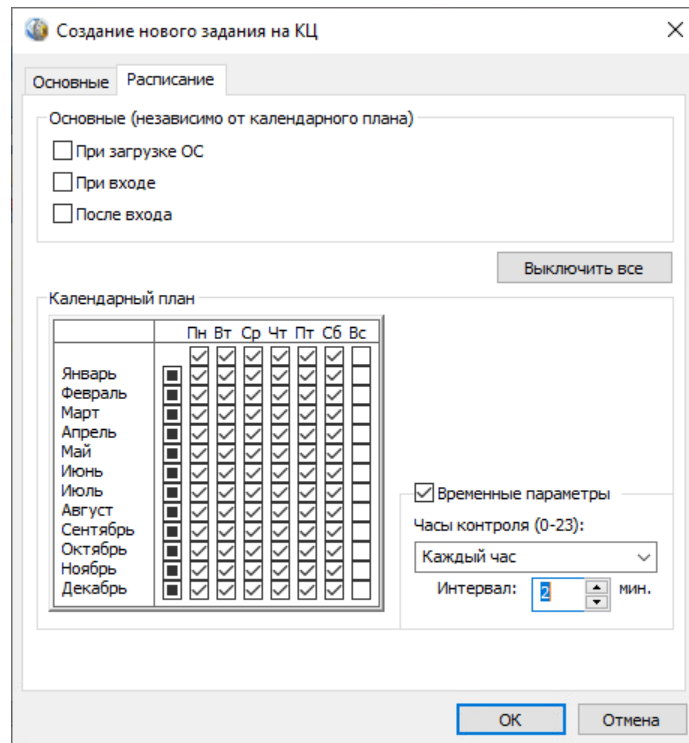
ОК Отмена

Алгоритм "Полное совпадение" предусматривает возможность восстановления контролируемого объекта в случае нарушения его целостности. Однако при использовании данного алгоритма существенно увеличивается объем базы данных, поскольку эталонным значением для контроля является копия объекта.

Обратите внимание, что в выпадающем списке "Алгоритм" в числе прочих есть возможность расчета контрольных сумм по ГОСТ Р 34.11-2012.

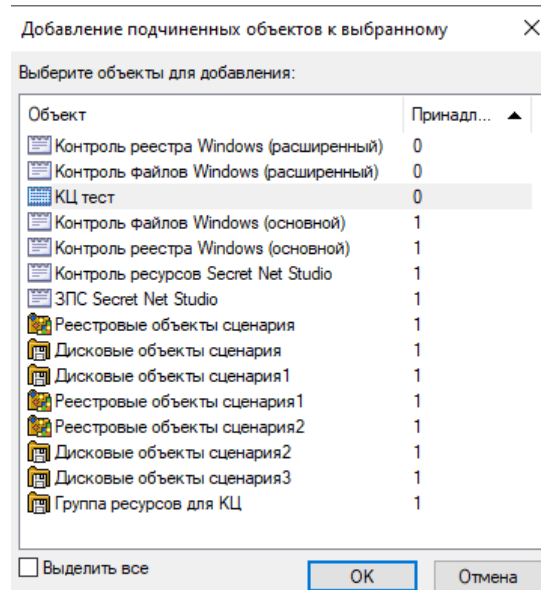
- перейдите на вкладку "Расписание" и в таблице "Календарный план" установите все отметки в верхней строке "Пн" – "Сб";
- в поле "Временные параметры" установите флажок, в поле "Часы контроля" выберите "Каждый час" и укажите интервал "2 мин.". Проверка целостности ресурса будет проводиться в заданные дни каждый час с интервалом 2 минуты.

Подробнее об установке параметров расписания см. в руководстве администратора по настройке и эксплуатации Secret Net Studio.

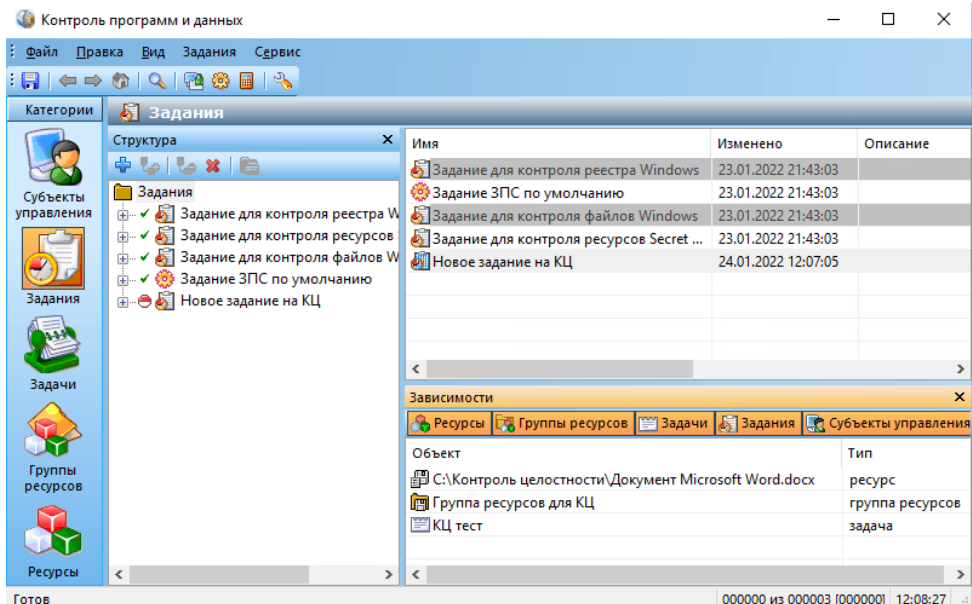


8. Нажмите кнопку "OK". В панели "Задания" сформируется новое задание "Новое задание на КЦ". Добавьте в созданное задание задачу "КЦ тест". Для этого:

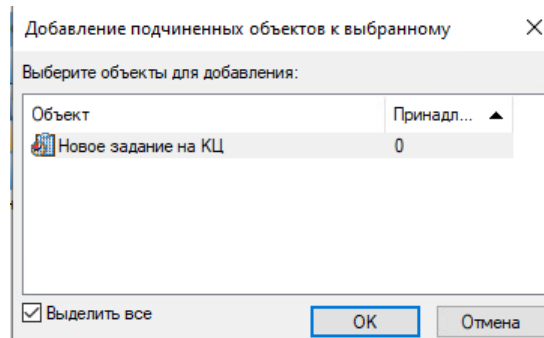
- в окне "Контроль программ и данных" для экземпляра задания "Новое задание на КЦ" вызовите контекстное меню и выберите опцию "Добавить задачи/группы / Существующие". Откроется диалоговое окно;



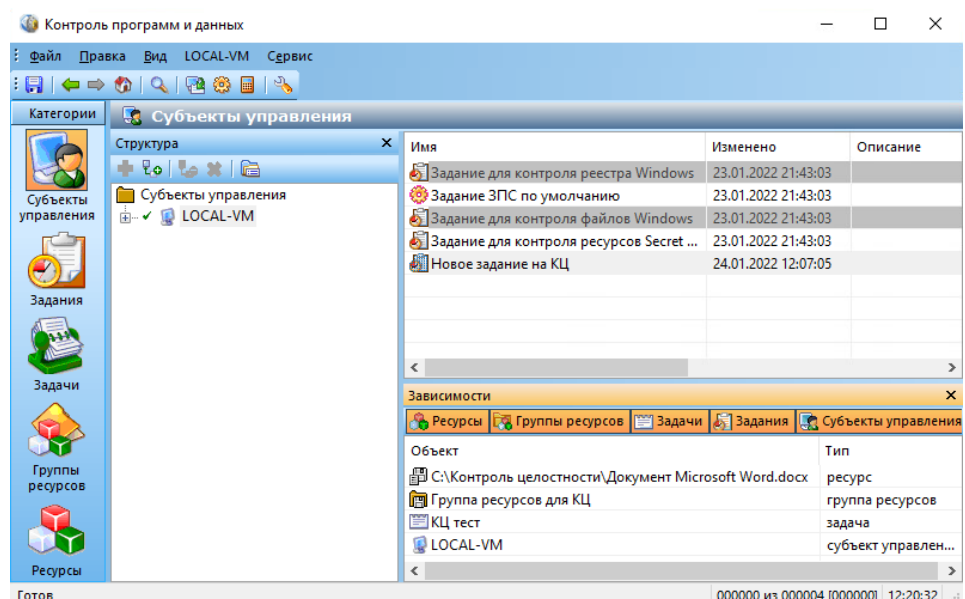
- выберите задачу "КЦ тест" и нажмите кнопку "OK". Вы вернулись в окно "Контроль программ и данных" и добавили задачу в задание.



9. Укажите субъект управления, на котором будет выполняться контроль целостности, т.е. выберите компьютер и добавьте к нему сформированное задание – при установке связи заданий контроля целостности с субъектами "Компьютер" или "Группа" (компьютеров) включается действие механизма КЦ. Для этого:
- в окне "Контроль программ и данных" выберите категорию "Субъекты управления" и для компьютера Local-VM из контекстного меню выберите опцию "Добавить задания / Существующие". Откроется диалоговое окно добавления объектов;

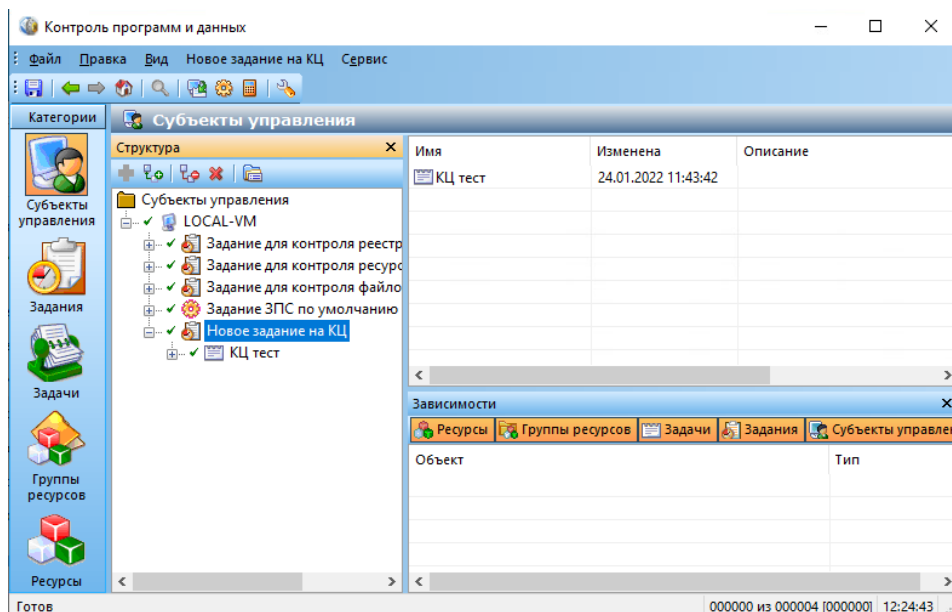


- выберите задание "Новое задание на КЦ" и нажмите кнопку "ОК". Задание добавлено субъекту.

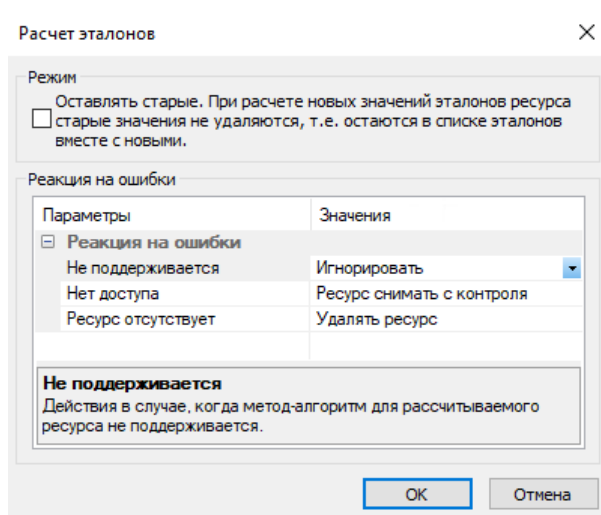


10. Проведите расчет эталонов для входящих в задания на КЦ контролируемых ресурсов. Для этого сделайте следующее:

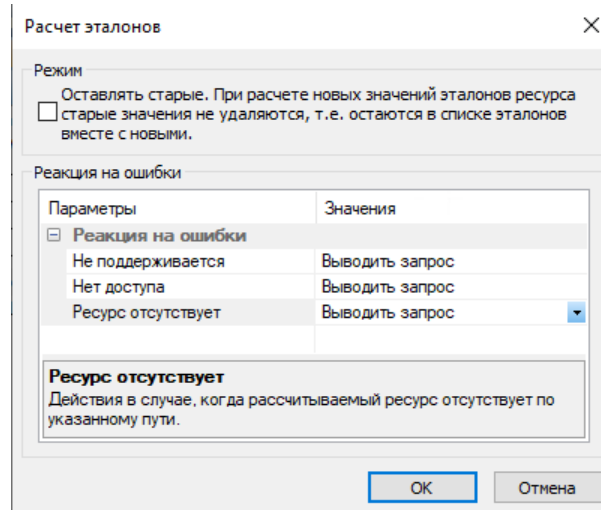
- в панели "Структура" разверните структуру субъекта управления "Local-VM", найдите и выделите задание "Новое задание на КЦ";



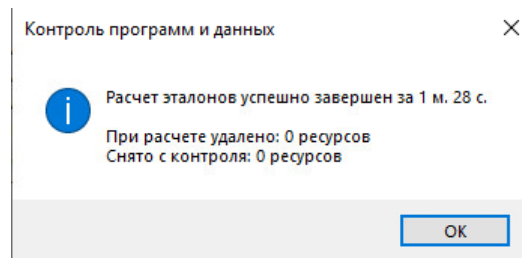
- в главном меню выберите опцию "Сервис / Эталон / Расчет". Откроется диалоговое окно "Расчет эталонов";



- в разделе "Реакция на ошибки" установите для всех пунктов значение "Выводить запрос" (система будет выводить соответствующее сообщение и запрос на выполнение последующих действий);



- нажмите кнопку "OK". В диалоговом окне подтверждения сохранения изменений нажмите кнопку "Да" и дождитесь окончания процесса расчета эталонов для ресурсов;



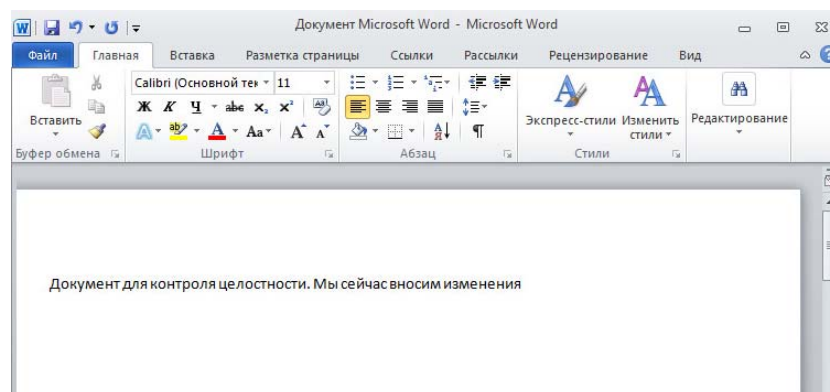
- после завершения расчета в окне информационного сообщения нажмите кнопку "OK". Вы вернетесь в окно программы "Контроль программ и данных".

11. Контроль целостности настроен.

Перед началом эксплуатации механизма КЦ можно выполнить проверку корректности параметров заданий. В связи с тем что в данном сценарии было сформировано достаточно простое задание, проводить такую проверку нет необходимости. Примите к сведению, что для ее начала используется команда "Запуск задания" из меню "Сервис".

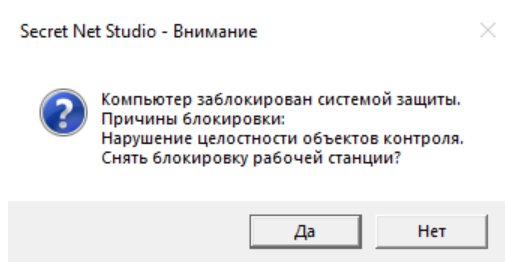
Далее будет проведена проверка работы механизма контроля целостности. Завершите работу программы "Контроль программ и данных", перезагрузите ВМ и авторизуйтесь под учетной записью "user1" (Иванов Иван Иванович).

12. Откройте файл "C:\Контроль целостности\Документ Microsoft Word.docx", внесите произвольные изменения, а затем сохраните и закройте документ.

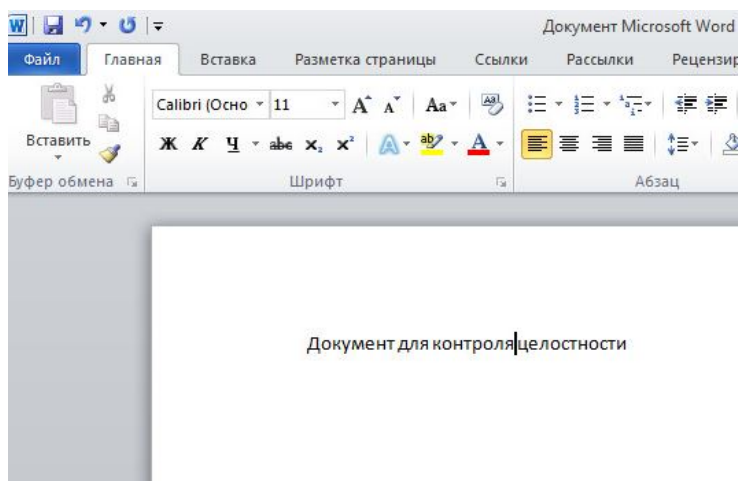


13. Подождите указанное в расписании контроля целостности время (см. п. 7, последний подпункт). Компьютер должен заблокироваться системой защиты Secret Net Studio.

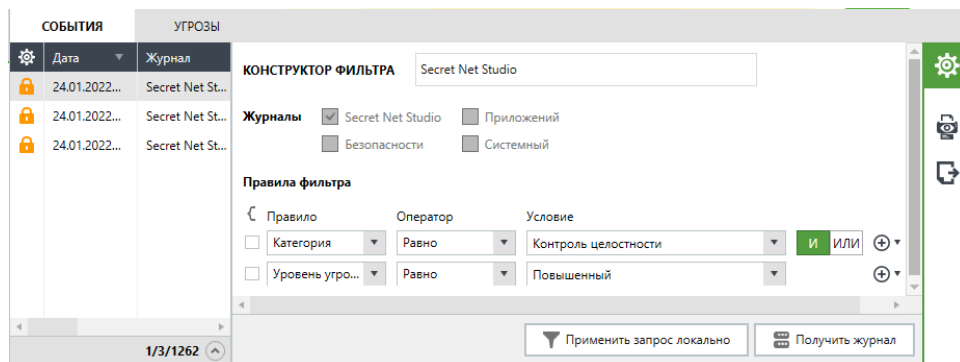
14. Войдите в систему под учетной записью "admin". В диалоговом окне ознакомьтесь с запросом на снятие блокировки.



15. Нажмите кнопку "Да", снимите блокировку и дождитесь окончания загрузки ОС.
16. Проверьте целостность файла "C:\Контроль целостности\Документ Microsoft Word.docx". Для этого откройте данный файл и убедитесь, что он восстановлен.



17. Запустите программу управления в локальном режиме, откройте журнал событий Secret Net Studio и найдите записи категории "Контроль целостности" с уровнем угрозы "Повышенный".



18. Проведена начальная настройка механизма КЦ и проверена его работа на примере контроля целостности текстового файла. Выполнение сценария завершено.

Сценарий №4 "Централизованное ведение журналов в Secret Net Studio"

В данном сценарии рассматривается проведение следующих операций по ведению журналов в Secret Net Studio:

- обработка событий тревоги (квитирование);
- сбор локальных журналов Secret Net Studio с защищаемых компьютеров в БД СБ;
- централизованная настройка на защищаемых компьютерах параметров локальных политик и регистрации определенных событий в журнале Secret Net Studio;
- настройка поиска угроз и просмотра сведений об угрозах.

1. Откройте консоль VM Admin_VM и убедитесь, что вы авторизованы в системе под учетной записью "snsadmin" (пароль "P@ssw0rd").
2. Запустите программу "Центр управления" и подключитесь к серверу безопасности SNS-Server.domain1.local. Данная программа предоставляет возможность контролировать и управлять состоянием и параметрами работы компьютеров, на которых установлено клиентское ПО системы Secret Net Studio в сетевом режиме, а также централизованно управлять параметрами групповых политик.

В окне программы управления вы увидите панель "Статистика", которая по умолчанию содержит фиксированный набор виджетов с настроенными параметрами для отображения сведений об общем состоянии защищенности системы.



3. Ознакомьтесь с виджетами панели "Статистика":
 - "Тревоги высокого уровня" – бордовый виджет, показывающий число несквитированных тревог высокого уровня;
 - "Тревоги повышенного уровня" – красный виджет, показывающий число несквитированных тревог повышенного уровня;
 - "Тревоги низкого уровня" – оранжевый виджет, показывающий число несквитированных тревог повышенного уровня;
 - "Запросы на утверждение АК" – синий виджет, показывающий количество компьютеров с запросом на утверждение аппаратной конфигурации;
 - "Ошибки лицензий" – белый виджет, показывающий количество компьютеров с нарушением лицензионной политики или истекшими лицензиями;
 - "Ошибки ФК" – красный виджет, показывающий количество компьютеров с ошибками выполнения функционального контроля;
 - "Заблокированные компьютеры" – красный виджет, показывающий количество заблокированных системой защиты компьютеров;
 - "Компьютеры с нарушением целостности" – белый виджет, показывающий компьютеры с наибольшим количеством зарегистрированных событий нарушения целостности при обработке заданий;
 - "Самые зараженные компьютеры" – белый виджет, показывающий компьютеры с наибольшим количеством зарегистрированных событий об обнаружении вируса;
 - виджеты могут содержать следующие элементы:

- числовой показатель актуальных событий, который является гиперссылкой, дающей возможность посмотреть информацию о данных событиях в соответствующем журнале;
- график распределения на интервале времени зарегистрированных событий. Столбик на графике является гиперссылкой, которая позволяет посмотреть информацию о событии в соответствующем журнале;
- список (перечень) имен защищаемых компьютеров. Имя является гиперссылкой, которая позволяет посмотреть информацию о защищаемом компьютере;
- "В журнал" – гиперссылка на все зарегистрированные в соответствующем журнале события, связанные с данным системным параметром и всеми контролируемыми объектами;
- пиктограмма  означает, что отображаются данные обо всех компьютерах, подчиненных серверу безопасности, включая компьютеры, подчиненные его дочерним серверам.

В панели управления указан период обновления информации виджетов

 Обновляется раз в 5 мин. Последнее обновление: 12:06

Примечание. Полный перечень виджетов с их описанием представлен в документе "Средство защиты информации Secret Net Studio. Руководство администратора. Установка, управление, мониторинг и аудит".

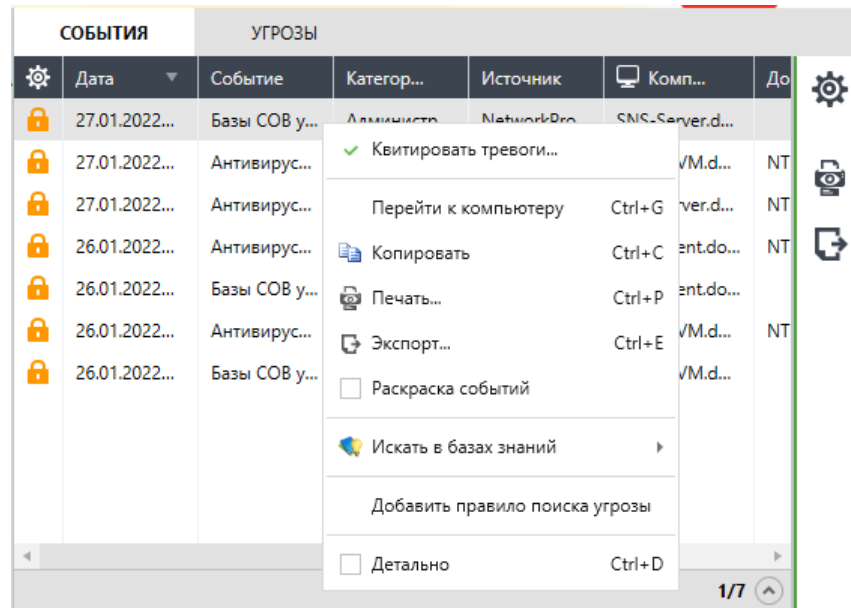
- Обратите внимание, что панель "События системы" в нижней части окна программы управления отображает информацию о происходящих событиях, о выполняемых командах или запросах пользователя и пр. Скрыть/показать данную панель, а также управлять фильтрацией вывода событий (системные, пользовательские или события тревоги) можно с помощью кнопок в правой нижней части.

Тип	Дата и время	Событие	Описание	41/41
	27.01.2022 13:01:45	Тревоги на станции. Компьютер: SNS-Server.domain1.local. T...	Получить описание тревоги.	
	27.01.2022 11:54:03	Тревоги на станции. Компьютер: Admin-VM.domain1.local. T...	Получить описание тревоги.	
	27.01.2022 11:53:59	На станцию Admin-VM.domain1.local зашел пользователь D...	Уведомление от агента.	
	27.01.2022 11:53:59	Admin-VM.domain1.local включен.	Уведомление от агента.	
	27.01.2022 11:53:26	Запрос конфигурации.	Конфигурация загружена.	

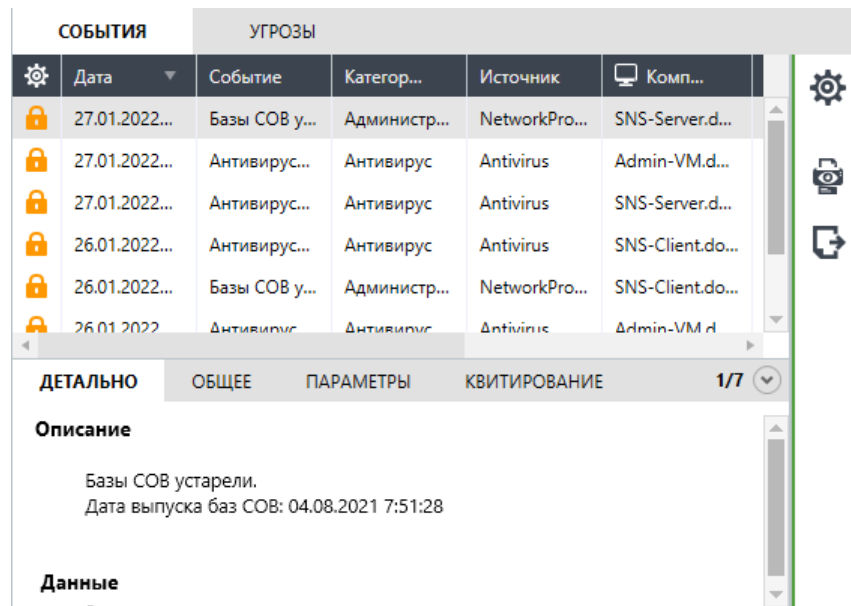
- Щелкните на любом ненулевом числовом индикаторе какого-либо виджета тревог – вы перейдете в журнал тревог. При этом автоматически сформируется и выполнится запрос на вывод событий тревог выбранного уровня (высокого, повышенного или низкого), после чего в панели событий появится запись о получении журнала тревог.

При получении уведомлений о произошедших событиях тревоги программа управления путем подачи различных визуальных сигналов незамедлительно оповещает об этом администратора безопасности.

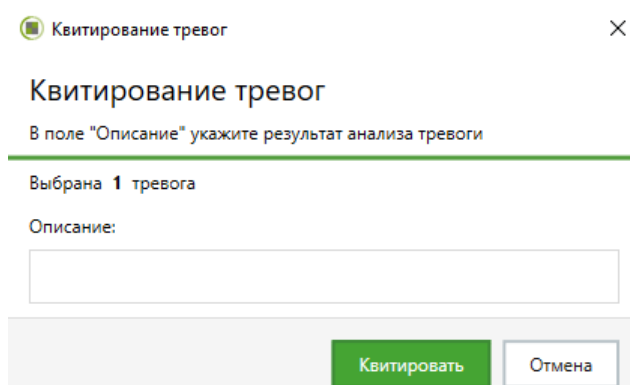
6. Выделите любое событие в журнале тревоги, вызовите его контекстное меню правой кнопкой мыши и последовательно ознакомьтесь с некоторыми возможными операциями над событиями, выбирая их из контекстного меню:



- "Детально" – отображение подробного описания событий;



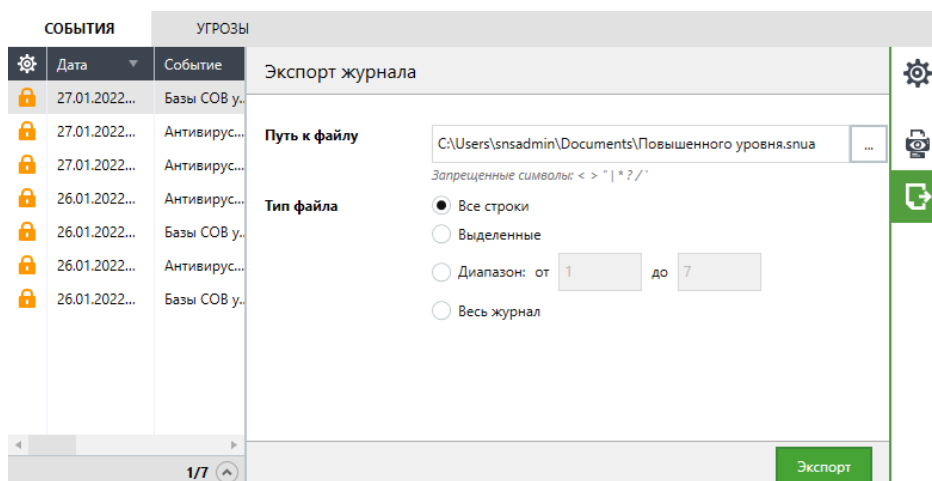
- "Квитировать тревоги". При этом администратор может ввести текстовый комментарий с описанием причин и принятых мер, и этот комментарий будет сохранен в системе вместе с признаком квитирования события. Информация о самом событии тревоги не удаляется из журнала. В дальнейшем по журналу событий тревоги можно определить, кто, когда и как отреагировал на произошедшие события. После квитирования всех полученных от компьютера событий для этого компьютера сбрасывается признак тревоги.



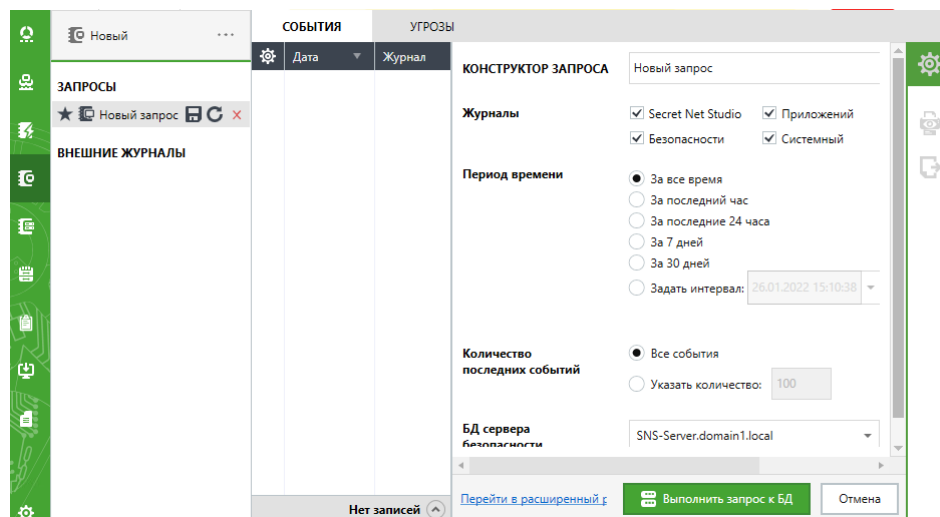
Квитировать можно отдельное событие или группу событий тревоги, предварительно выделив их с помощью клавиш [Ctrl] или [Shift];

Примечание. Помимо квитирования событий тревоги с обязательным вводом комментария администратором безопасности, в программе предусмотрена возможность сброса счетчиков событий. Эта процедура предназначена только для случаев, связанных с настройкой системы защиты, и не должна применяться в штатном режиме функционирования.

- "Экспорт". Позволяет экспортировать (сохранять) записи текущего запроса в файлы специальных форматов: *.snua – записи журнала событий тревоги; *.snlog – записи журнала станций; *.snsrv – записи журнала сервера безопасности. Эта операция может также выполняться с помощью кнопки "Экспорт журнала" , расположенной в правой части окна.



7. В панели навигации нажмите кнопку "Журналы станций" , сформируйте общий запрос на показ записей из всех журналов и убедитесь, что результат его будет пустым.

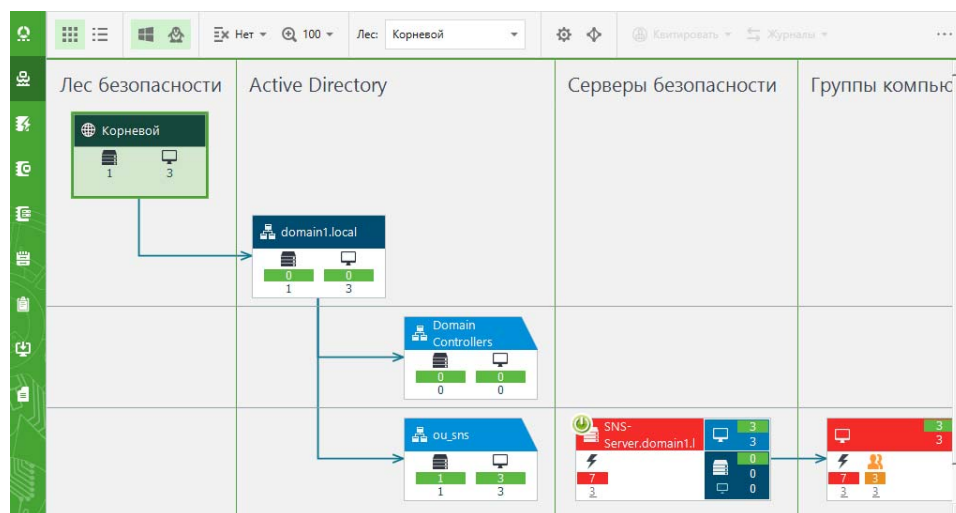


Журнал станций – это объединенный журнал компьютеров, который предназначен для централизованного хранения содержимого локальных журналов (журнал Secret Net Studio и штатные журналы ОС Windows), поступивших с защищаемых компьютеров.

Пустой результат запроса означает, что в базе данных сервера безопасности нет полученных с защищаемых компьютеров записей, которые удовлетворяют заданным в запросе правилам отбора.

8. В ПУ откройте панель "Компьютеры"  и выберите представление "Диаграмма", которое, как уже ранее отмечалось, отображает леса безопасности, домены, организационные подразделения, серверы безопасности и группы компьютеров, подчиненные серверам безопасности.

Ознакомьтесь с некоторыми используемыми в диаграмме управления значками:



 – сервер безопасности, с которым установлено соединение (сервер подключения как объект групповой политики);

 – включена блокировка компьютера (компьютеров). Число показывает количество причин блокировки;

 – на компьютере (компьютерах) обнаружен вирус. Число показывает количество зарегистрированных событий обнаружения вирусов;

 – счетчик зарегистрированных событий тревоги, ожидающих квитирования (подтверждение приема) администратором безопасности. Максимальное числовое значение счетчика – 999. В случае превышения ограничения счетчик отображает значение "99+";



1 3 – количество открытых на компьютерах сессий работы пользователей. Оранжевый цвет значка и фона обозначает сессию локального администратора;



– на компьютере (компьютерах) действует фильтр событий тревоги;



ЛЦ – зафиксирована ошибка (красный цвет) или предупреждение (желтый цвет) при проверке лицензии;



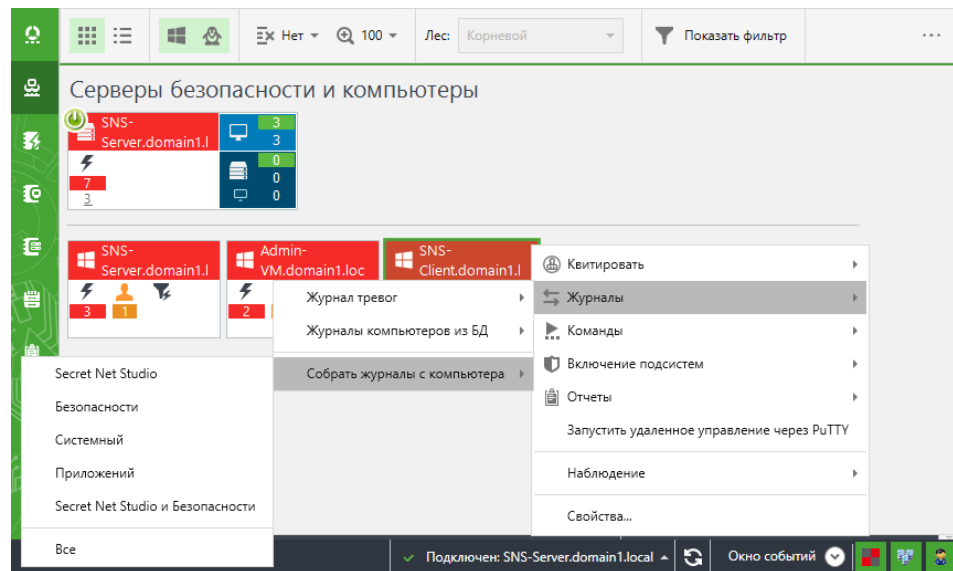
– БД сервера безопасности переполнена;



OFF – учетная запись компьютера отключена.

9. Проведите процедуру сбора журналов с компьютера SNS-Client. Для этого:

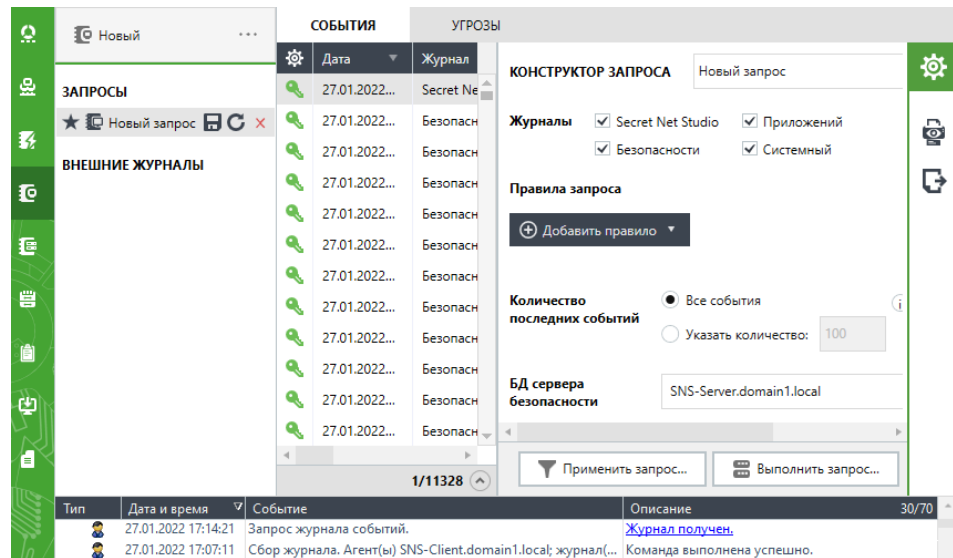
- в диаграмме управления раскройте двойным щелчком группу компьютеров. Обратите внимание, что при этом выбираются (помечаются) все содержащиеся в данной группе компьютеры;
- выберите плитку компьютера SNS-Client. Правой кнопкой мыши вызовите ее контекстное меню и выберите опцию: "Журналы / Собрать журналы с компьютера / Все";



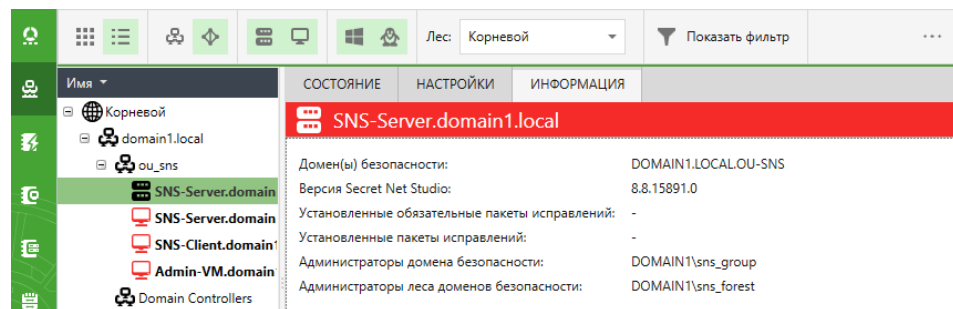
- обратите внимание на сообщение о сборе журнала в панели событий системы и дождитесь завершения операции сбора – в поле "Описание" этого события появится отметка "Команда выполнена успешно";

Тип	Дата и время	Событие	Описание	27/67
	27.01.2022 17:07:11	Сбор журнала. Агент(ы) SNS-Client.domain1.local; журнал(...)	Команда выполнена успешно.	
	27.01.2022 16:54:01	Запрос конфигурации.	Конфигурация загружена.	

- в панели навигации нажмите кнопку "Журналы станций" и повторите выполнение запроса, который вы сформировали в п. 7 (см. выше);
- ознакомьтесь с результатами данной операции. Поскольку мы провели процедуру сбора журналов, в БД сервера безопасности теперь есть записи, полученные с защищаемых компьютеров.

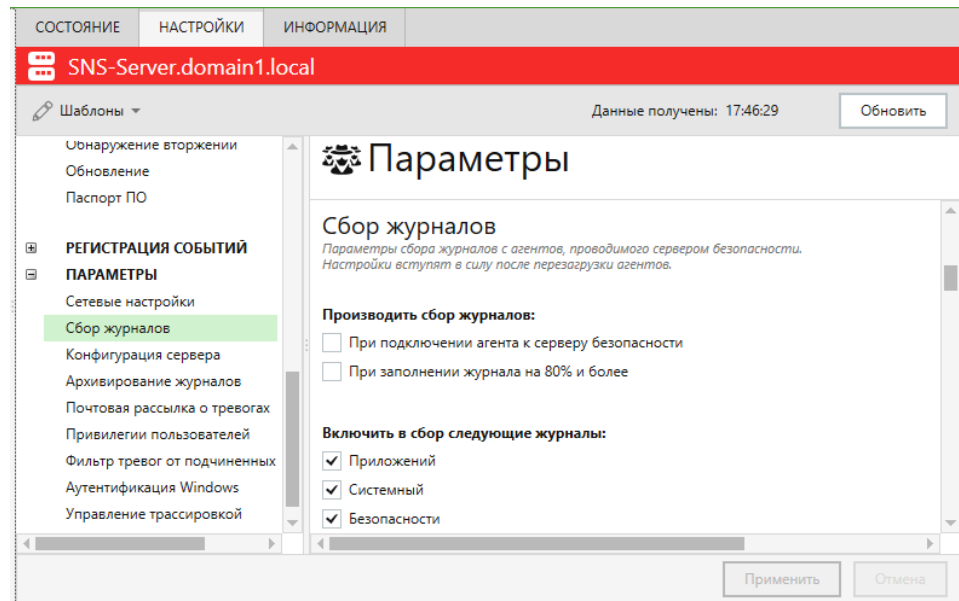


10. Ознакомьтесь с возможностью централизованной настройки параметров передачи локальных журналов в БД СБ. Для этого в ПУ откройте панель "Компьютеры" , в диаграмме управления выберите элемент сервера безопасности, который отмечен значком , и, используя опцию "Свойства" из его контекстного меню или кнопку "Свойства"  в панели управления, раскройте окно свойств и выберите вкладку "Информация". Просмотрите общие сведения о домене безопасности.



11. Переключитесь на вкладку "Настройки". Если на этой вкладке появится кнопка "Загрузить настройки", нажмите ее, чтобы загрузить параметры настроек выбранного объекта.

В левой части окна раскройте раздел "Параметры" и выберите группу параметров "Сбор журналов", которая содержит параметры передачи локальных журналов на сервер безопасности.



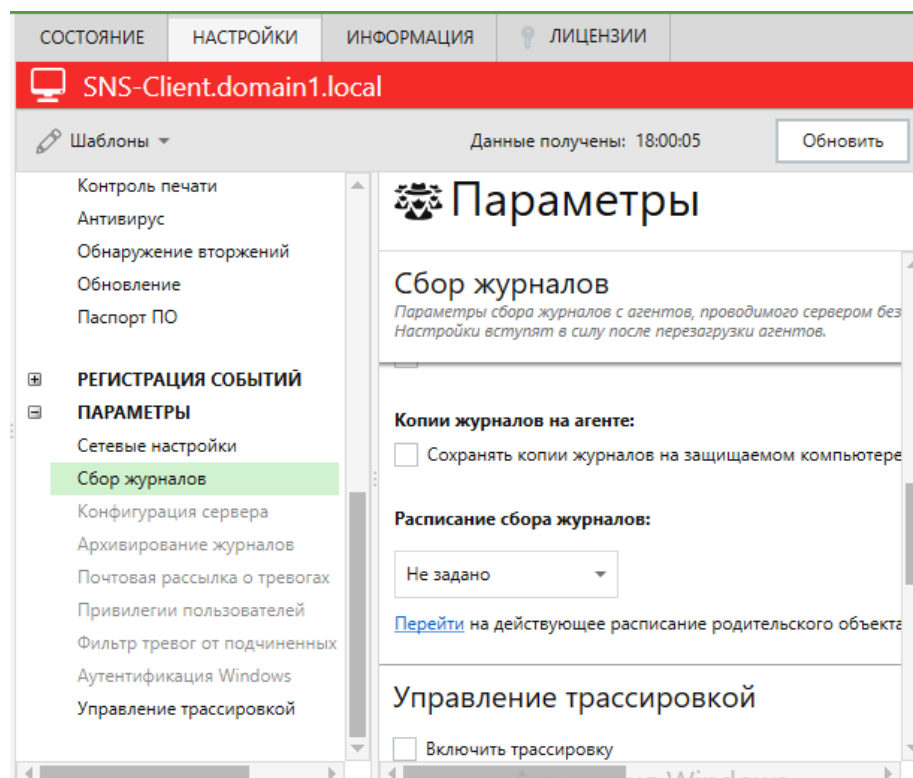
12. Параметры сбора локальных журналов, заданные для сервера безопасности, относятся ко всем компьютерам, которые подчинены этому серверу. На отдельных компьютерах можно настроить индивидуальные параметры, которые будут иметь более высокий приоритет по сравнению с заданными на СБ параметрами. Установите следующие параметры сбора локальных журналов:

- в группе настроек "Производить сбор журналов" установите флажок в поле "При подключении агента к серверу безопасности";
- обратите внимание на поле "Сохранять копии журналов на защищаемом компьютере" – его следует использовать, если требуется оставлять на рабочих станциях копии содержимого локальных журналов после их передачи на сервер безопасности. Эти копии сохраняются на компьютере в evt-файлах в каталоге "%ProgramData%\ Security Code\ Secret Net Studio\ Client\ OmsAgentEvtCopy". Обработка и удаление данных файлов должна выполняться администратором;
- в группе "Включить в сбор следующие журналы" снимите флажок в поле "Системный".

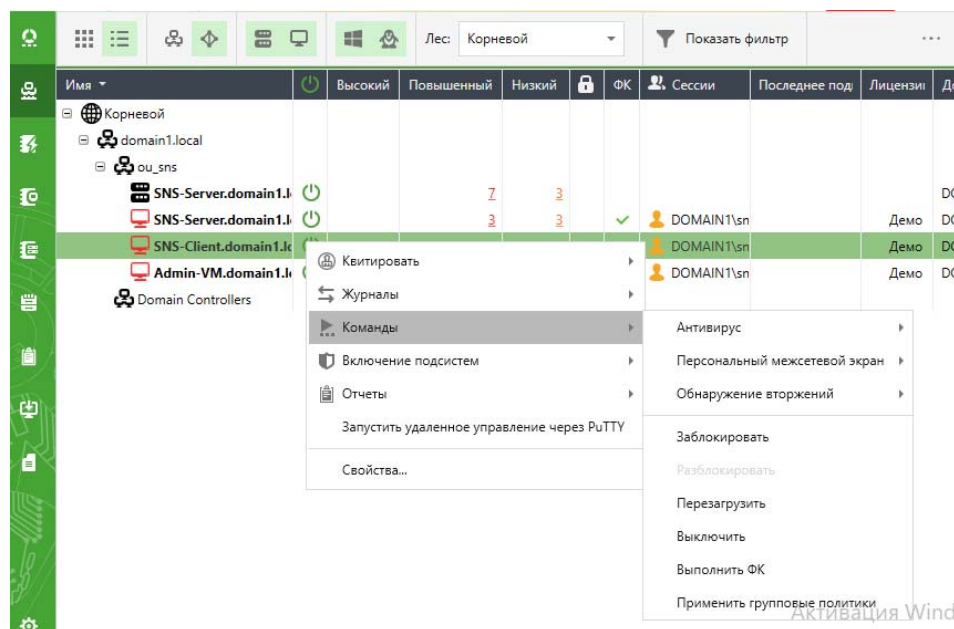
13. Нажмите кнопку "Применить" и дождитесь завершения процедуры сохранения параметров. В панели событий системы появится соответствующая запись о сохранении конфигурации.

Тип	Дата и время	Событие	Описание	40/77
	27.01.2022 17:55:30	Сохранение конфигурации ОУ.	Конфигурация сохранена.	
	27.01.2022 17:54:50	Запрос конфигурации.	Конфигурация загружена.	

14. В панели "Компьютеры" выберите агент SNS-Client, на вкладке "Настройка" раскройте раздел "Параметры" и выберите группу параметров "Сбор журналов". В данном режиме можно настроить индивидуальные локальные настройки сбора журналов, которые будут иметь более высокий приоритет по сравнению с заданными на СБ параметрами. Обратите внимание, что для компьютера SNS-Client текущие настройки сбора журналов не менялись и отличаются от заданных в пп. 11–13 для сервера безопасности. Убедитесь, что в раскрывающемся списке для выбора расписания сбора журналов установлено "Не задано", и выберите ссылку "Перейти на действующее расписание родительского объекта" – вы снова вернетесь к установленным для СБ настройкам сбора журналов.

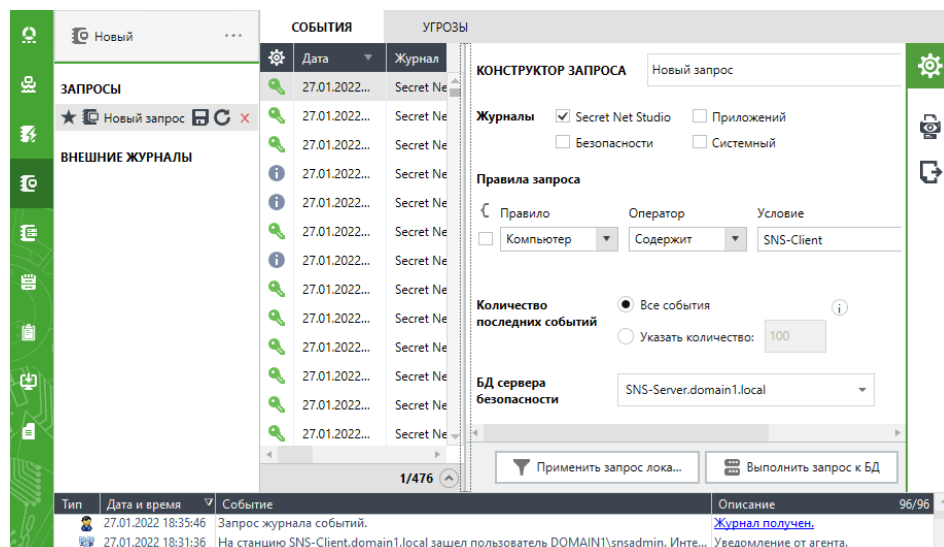


15. Используя кнопку "Свойства" , закройте панель свойств и вернитесь к интерфейсу таблицы или диаграммы управления. Вызовите контекстное меню агента SNS-Client и выберите опцию "Команды / Перезагрузить". В диалоговом окне подтверждения перезагрузки нажмите кнопку "Да". Дождитесь завершения перезагрузки и авторизуйтесь на ВМ компьютера SNS-Client под учетной записью "snsadmin".

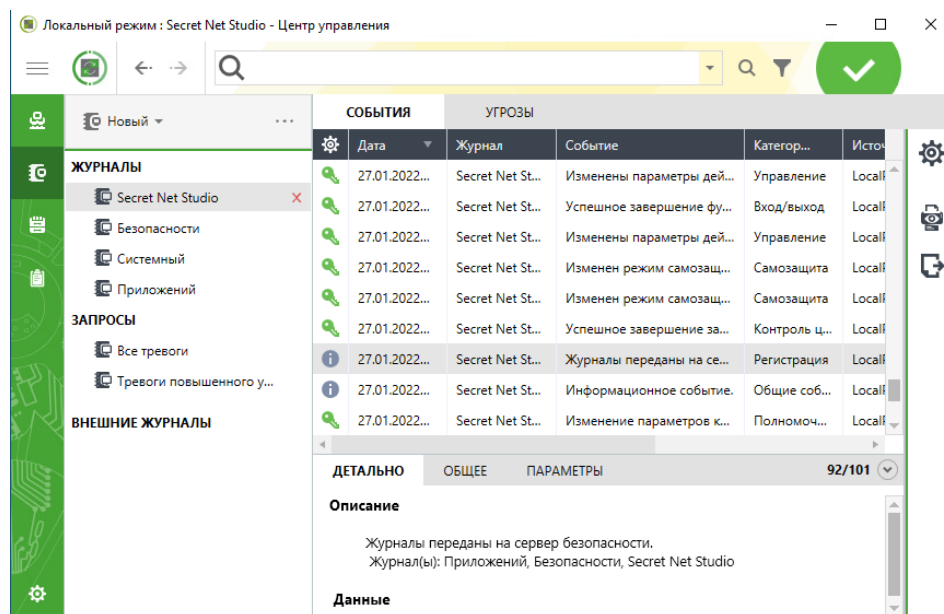


16. Обратите внимание, что в панели событий системы появились записи об успешной перезагрузке и авторизации пользователя в системе.
17. Используя описание п. 7, раскройте панель "Журналы станций" , сформируйте соответствующий запрос и убедитесь, что после перезагрузки защищаемого компьютера SNS-Client и подключения агента к СБ содержимое локальных журналов, кроме системного, было передано с SNS-Client в БД СБ. Обратите внимание на панель событий системы, в которой отражены записи о запросе журнала с пометкой о получении в поле "Описание".

Примечание. Параметры расписания, заданные для сервера безопасности, не применяются на защищаемых компьютерах с индивидуально настроенными расписаниями передачи журналов.



- 18.** Переключитесь в окно BM SNS_Client, запустите программу "Локальный центр управления", откройте панель "Журналы"  и с помощью соответствующих запросов убедитесь, что после перезапуска были переданы в БД СБ и соответственно очищены все локальные журналы, кроме системного. Убедитесь, что системный журнал содержит все записи с момента последней принудительной передачи их на сервер безопасности (см. п.9).



СОБЫТИЯ		УГРОЗЫ			
Дата	Журнал	Событие	Категор...	Источник	Имя источника
27.01.2022 23:37...	Системный	10016		Microsoft...	SNS
27.01.2022 23:32...	Системный	16		Microsoft...	SNS
27.01.2022 23:32...	Системный	7001	(1101)	Microsoft...	SNS
27.01.2022 23:31...	Системный	104	Очистка жу...	Microsoft...	SNS
27.01.2022 23:30...	Системный	16		Microsoft...	SNS
27.01.2022 23:30...	Системный	10016		Microsoft...	SNS
27.01.2022 23:30...	Системный	16		Microsoft...	SNS
27.01.2022 23:29...	Системный	7026		Service Con...	SNS
27.01.2022 23:29...	Системный	35		Microsoft...	SNS
27.01.2022 23:29...	Системный	1014	(1014)	Microsoft...	SNS
27.01.2022 23:29...	Системный	37		Microsoft...	SNS
27.01.2022 23:29...	Системный	4		Microsoft...	SNS
27.01.2022 23:29...	Системный	1		Microsoft...	SNS

Подробнее об обработке событий журнала тревог и других журналов см. в документе "Средство защиты информации Secret Net Studio. Руководство администратора. Установка, управление, мониторинг и аудит".

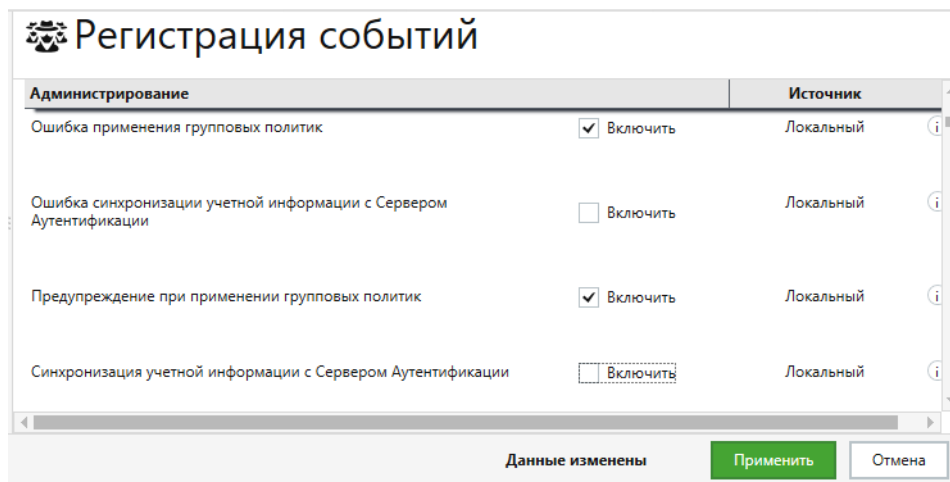
19. Операции квитирования тревог и сбора локальных журналов рассмотрены. Далее будет рассмотрен пример централизованной сетевой настройки на защищаемых компьютерах параметров локальных политик и регистрации определенных событий в журнале Secret Net Studio (в сценарии №2 уже показывалась автономная настройка для отдельного компьютера параметров раздела "Регистрация событий" и группы "Политики / Базовая защита").

В окне консоли VM Admin_VM, в панели "Компьютеры" программы управле-

ния через кнопку "Свойства"  откройте панель свойств компьютера SNS-Client и на вкладке "Настройки" раскройте группу "Регистрация событий / Администрирование".

Администрирование	Источник
Включена защитная подсистема	Локальный
Групповые политики успешно применены	Локальный
Добавлен пользователь	Локальный
Закрыта локальная программа управления	Локальный

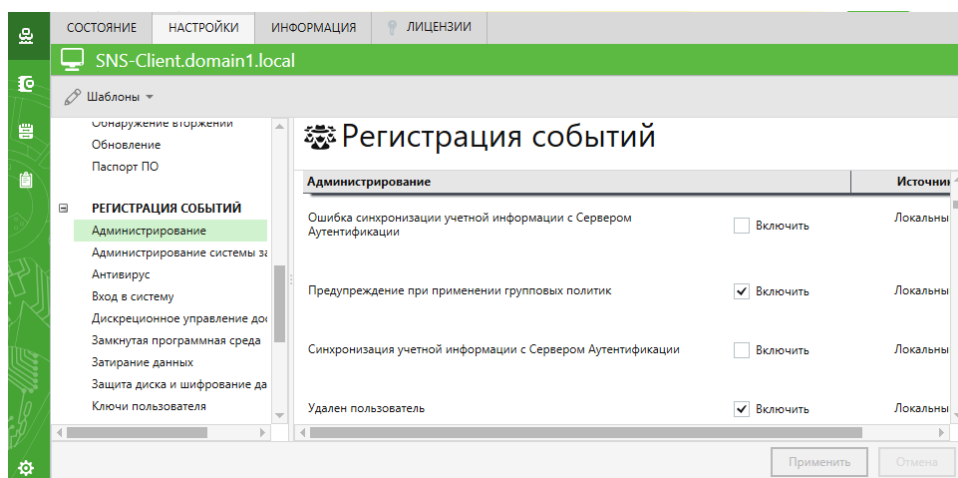
Найдите и отключите параметры "Ошибка синхронизации учетной информации с Сервером Аутентификации" и "Синхронизация учетной информации с Сервером Аутентификации".



20. Нажмите кнопку "Применить", дождитесь появления в панели событий системы записей об успешном выполнении команды и изменении локальных политик на агенте.

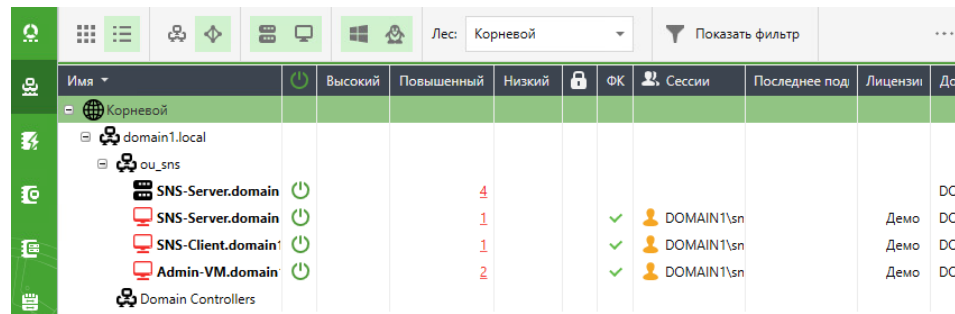
Тип	Дата и время	Событие	Описание	186/186
	31.01.2022 18:02:27	На агенте SNS-Client.domain1.local изменились политики.	Уведомление от агента.	
	31.01.2022 18:02:09	Применение политик для агента(ов) 'SNS-Client.domain1.local'.	Команда выполнена успешно.	

21. Переключитесь в окно BM SNS-Client. В программе "Локальный центр управления" выберите панель "Компьютер", раскройте вкладку "Настройки", разверните группу параметров "Регистрация событий / Администрирование" и убедитесь, что регистрация событий "Ошибка синхронизации учетной информации с Сервером Аутентификации" и "Синхронизация учетной информации с Сервером Аутентификации" отключена.

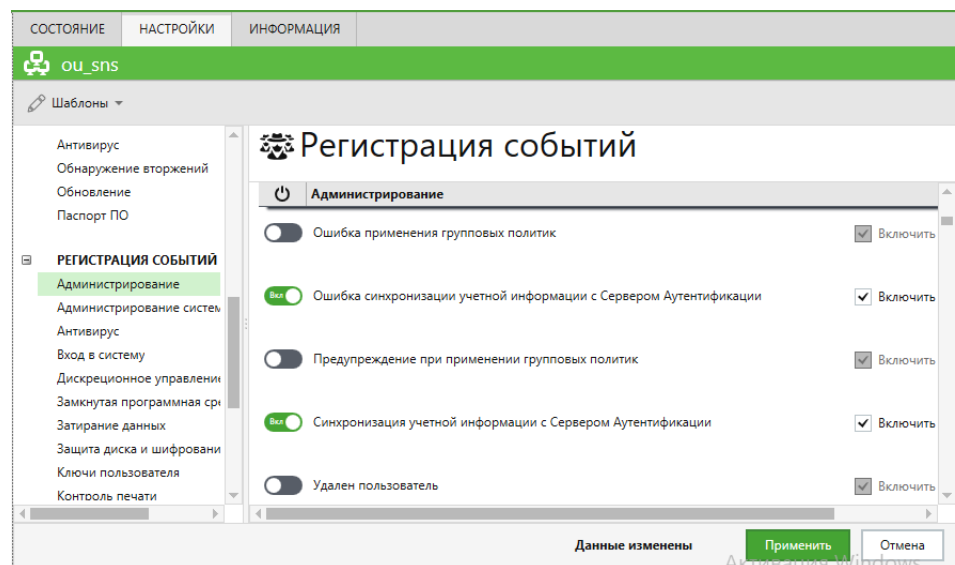


22. Теперь изменим данные параметры для всего домена безопасности, т.е. в нашем случае для подразделения "ou_sns":

- переключитесь в окно консоли BM Admin_VM, в панели "Компьютеры" программы управления с помощью кнопки "Свойства"  сверните панель свойств компьютера SNS-Client. На текущей вкладке будет отображена таблица управления со списком компьютеров;
- убедитесь, что в панели навигации в верхней части окна кнопка "Структура AD"  находится в нажатом состоянии (выделена цветом), и поэтому на текущей вкладке отображаются домены Active Directory, организационные подразделения, серверы безопасности и подчиненные им компьютеры;



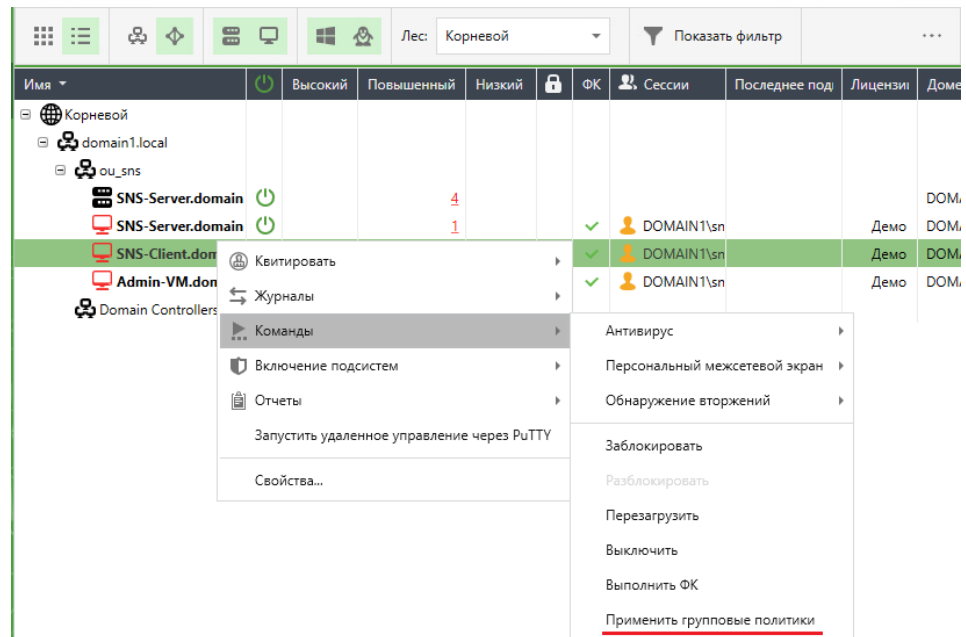
- выберите организационное подразделение "ou_sns", на которое был спроецирован домен безопасности, с помощью кнопки "Свойства" откройте панель его свойств и переключитесь на вкладку "Настройки". Если появится кнопка "Загрузить настройки", нажмите ее, чтобы загрузить параметры настроек выбранного объекта;
- в группе политик "Регистрация событий / Администрирование" с помощью значка включите параметры "Ошибка синхронизации учетной информации с Сервером Аутентификации" и "Синхронизация учетной информации с Сервером Аутентификации";



- нажмите кнопку "Применить". В панели событий появится запись об успешном сохранении конфигурации и применении политик.

Тип	Дата и время	Событие	Описание	199/199
	01.02.2022 13:49:05	Применение политик для 'ou_sns'.	Конфигурация сохранена.	

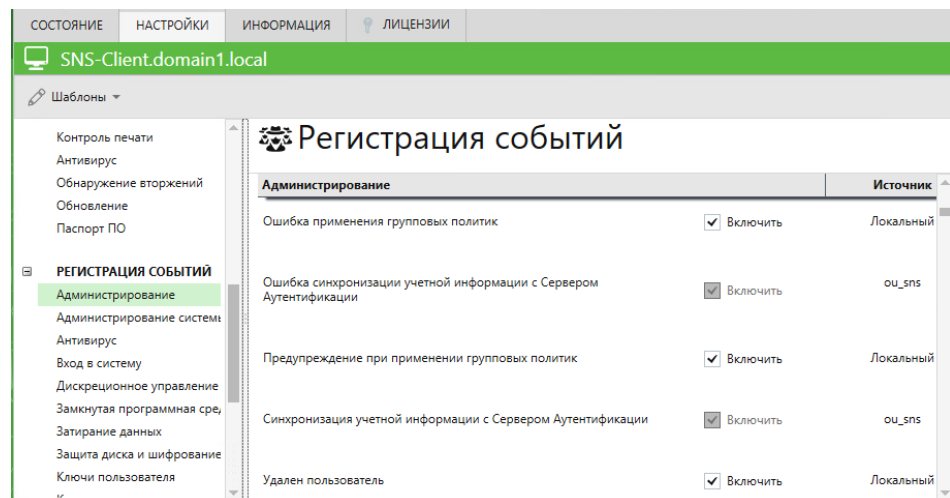
23. С помощью кнопки "Свойства" закройте окно свойств организационного подразделения. На текущей вкладке будет отображена таблица управления со списком компьютеров. Раскройте контекстное меню компьютера SNS-Client и выберите опцию "Команды / Применить групповые политики".



24. Обратите внимание на сообщение в панели событий об успешном применении на агенте групповых политик.

Тип	Дата и время	Событие	Описание
01.02.2022 14:14:21	Команда 'Применить групповые политики' отправлена для агента(ов) 'SNS-Client....'	Команда выполнена успешно.	202/202

25. Переключитесь в окно консоли BM SNS-Client и в программе управления в локальном режиме убедитесь, что регистрация событий "Ошибка синхронизации учетной информации с Сервером Аутентификации" и "Синхронизация учетной информации с Сервером Аутентификации" включена на уровне организационного подразделения и в локальном режиме не изменяется.



Параметры политик, заданные для корневого сервера безопасности, имеют наивысший приоритет и применяются на всех компьютерах, которые находятся в непосредственном или транзитивном подчинении.

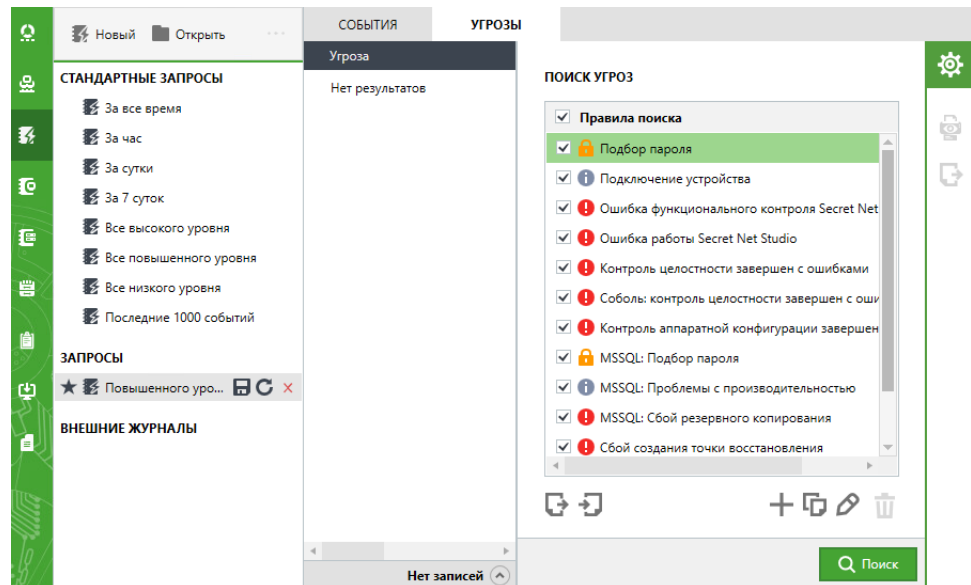
По умолчанию параметры заданы только в локальной политике. Для большинства параметров локальной политики изменение значений возможно как централизованно в программе управления, так и локально на защищаемом компьютере. При этом изменить в локальной политике значение, заданное политикой другого уровня, невозможно. Сведения о политике, определяющей значение параметра, представлены в таблице локальных политик в колонке "Источник".

26. Ознакомьтесь с настройками поиска событий угроз и проведите просмотр списка угроз, полученного в результате анализа загруженных записей журналов. Следует помнить, что режим просмотра угроз предназначен для предоставления администратору или аудитору наиболее важной для них информации из журналов, а сами события угроз представляют собой сжатые

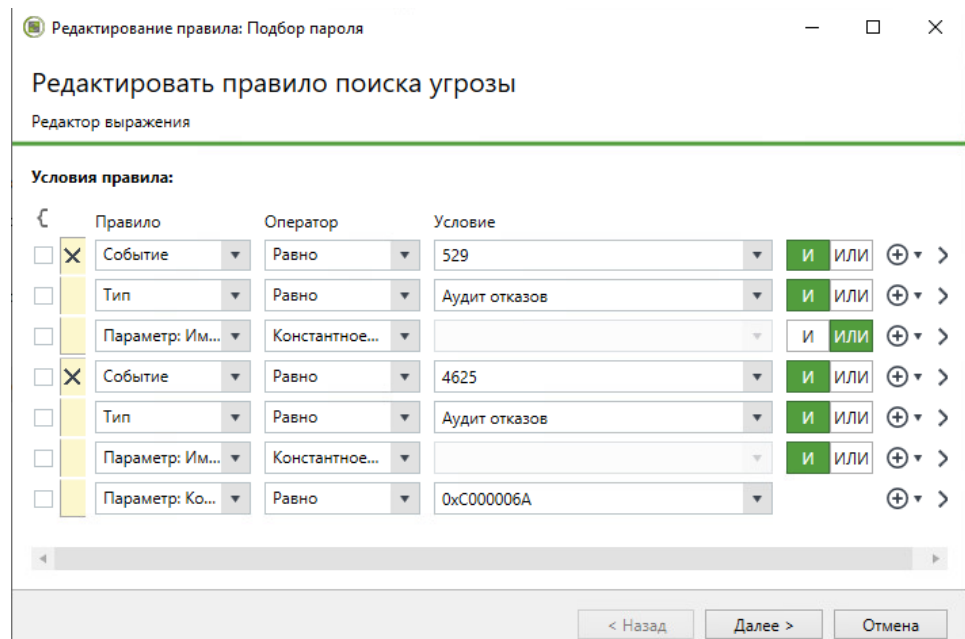
или разъясняющие сведения о зарегистрированных событиях (например, событиях с признаками подбора пароля).

Для настройки поиска событий угроз выполните следующие действия:

- в панели навигации нажмите кнопку "Журнал тревог" , в области отображения сведений переключитесь на вкладку "Угрозы" и справа от области отображения сведений нажмите кнопку "Запрос" . Откроется панель настройки параметров поиска угроз, содержащая предустановленные по умолчанию правила общего характера, которые нельзя удалять или изменять, но можно на их основе создать собственные правила (через кнопку "Копировать" );



- просмотрите полученный список. Убедитесь, что выбрано правило поиска "Подбор пароля" и под списком правил справа нажмите кнопку "Редактировать правило угрозы" . Откроется диалоговое окно "Редактирование правила: ...", где можно только просматривать заданные условия для выбранного стандартного правила, которым должны удовлетворять записи для соответствия данному событию угрозы;

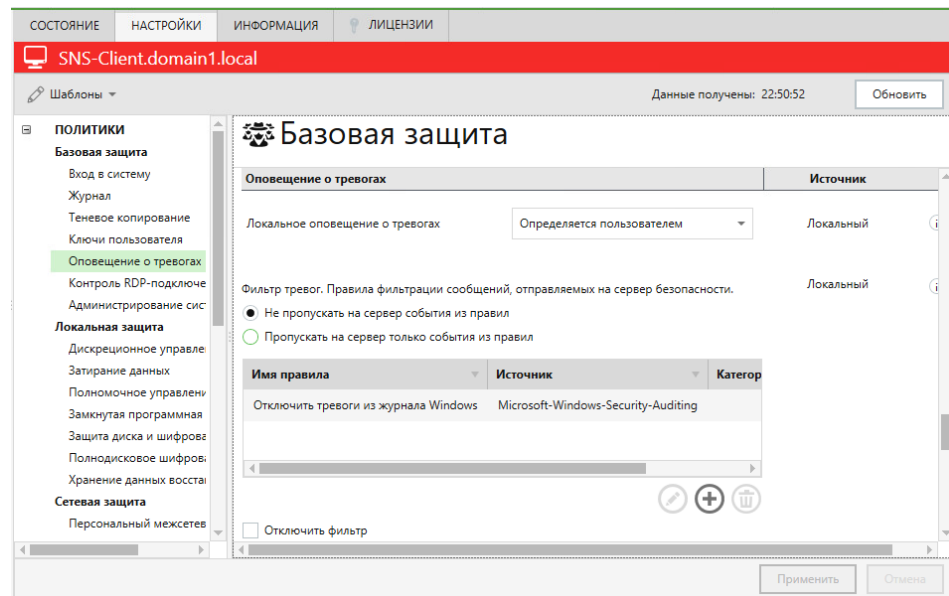


- просмотрите список условий выбранного правила. Обычно он содержит несколько связанных между собой выражений. Связь формируется с по-

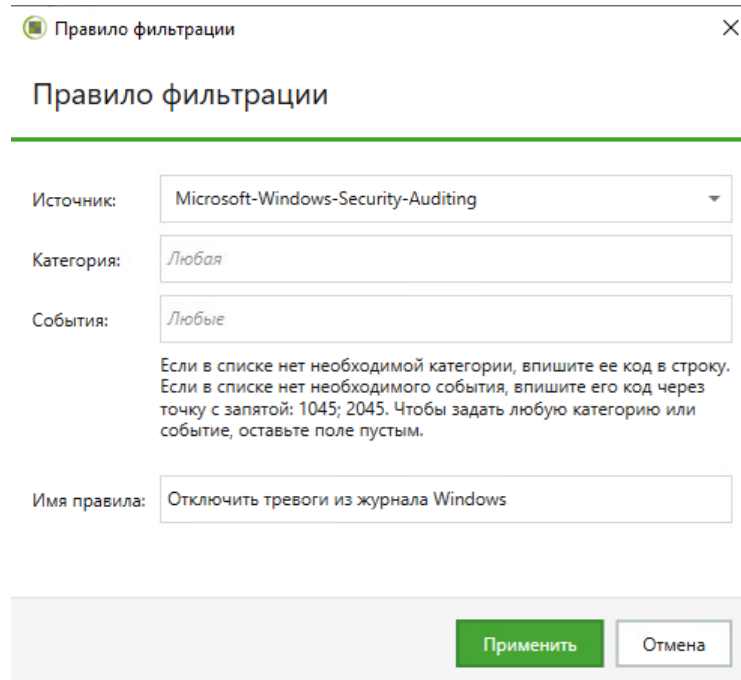
мощью логических операторов И/ИЛИ либо значка группировки (кнопка с фигурной скобкой над списком). Группировка позволяет задать обязательное совпадение заданных значений для полей (например, "Тип", "Событие" и "Параметр: Имя пользователя"), чтобы при анализе не рассматривались записи, у которых хотя бы одно из значений в указанных полях не совпадает с заданным;

- нажмите кнопку "Далее". В данном окне мастера показаны дополнительные параметры правила: выбрать журналы, записи которых будут рассматриваться при анализе, для отслеживания повторяющихся событий указать количество повторов в интервале времени, а также выбрать режим сжатия в поле "фиксировать одну тревогу за сессию пользователя", чтобы при выявлении нескольких одинаковых событий за сеанс работы пользователя в журнале формировать только одну запись;

- обратите внимание, что для формирования события тревоги и соответствующей угрозы задано 3 попытки ввода пароля. Нажмите кнопку "Отмена". Самостоятельно просмотрите условия и параметры поиска других правил, например, "Контроль целостности завершен с ошибками".
- 27.** Перед просмотром списка угроз ознакомьтесь с возможностью установки непосредственно на защищаемых компьютерах фильтра передачи уведомлений о событиях тревоги. Для этого:
- в панели навигации переключитесь на панель "Компьютеры", выберите компьютер SNS-Client, раскройте панель его свойств и на вкладке "Настройки" разверните группу "Политики / Базовая защита / Оповещение о тревогах". Данные параметры позволяют ограничить непосредственно на защищаемых компьютерах передачу на СБ уведомлений о событиях тревоги;



- с помощью значка-кнопки  ознакомьтесь с описанием параметров выбранной политики и обратите внимание, что по умолчанию заданы значения: "Локальное оповещение о тревогах" – "Определяется пользователем", "Фильтр тревог. Правила фильтрации сообщений ..." – "Не пропускать на сервер события из правил". В заданных настройках фильтр не пропускает уведомления о событиях тревоги, которые удовлетворяют условиям правил в таблице;
- выберите в таблице запись от источника "Microsoft-Windows-Security-Auditing" и под таблицей нажмите кнопку "Редактировать" . Откроется диалоговое окно для настройки параметров выбранного правила;



- параметры правил фильтрации уведомлений настраиваются аналогично параметрам фильтра тревог от подчиненных серверов и подробно описаны в документе "Средство защиты информации Secret Net Studio. Руководство администратора. Установка, управление, мониторинг и аудит":
 - "Источник" – имя компонента/подсистемы – источника события;
 - "Категория" – числовой код категории событий;
 - "Событие" – числовые идентификаторы событий;

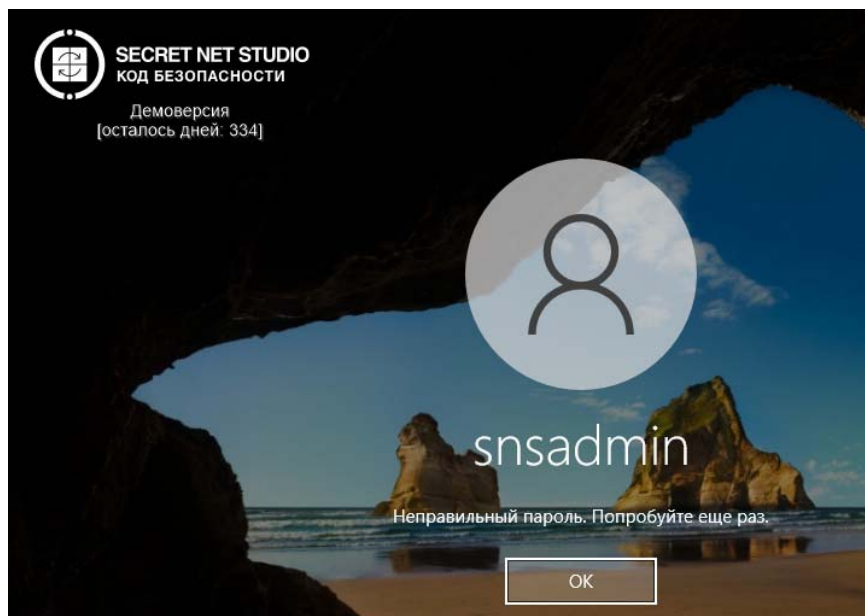
- в диалоговом окне "Правило фильтрации" нажмите кнопку "Отмена". В параметрах группы политик "Оповещение о тревогах" установите переключатель "Отключить фильтр" и нажмите кнопку "Применить";

Примечание. Не включайте инверсный режим "Пропускать на сервер только события из правил" при пустом списке правил. Иначе фильтр не пропустит ни одно событие тревоги.

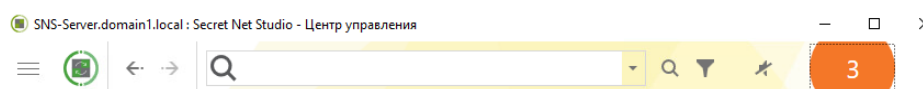
- убедитесь, что в панели событий появилась запись об изменении политик на агенте SNS-Client.

28. Просмотрите сформированный на основе заданных в п. 27 настроек список угроз. Для этого:

- используя описание п. 6, проведите квитиование всех имеющихся событий тревоги и убедитесь, что журнал тревог теперь пуст;
- переключитесь в окно VM SNS_Client и переавторизуйтесь под УЗ snsadmin, указав три раза неправильный пароль;



- переключитесь в окно VM Admin_VM. Обратите внимание на изменившийся числовой показатель индикатора тревог в правом верхнем углу окна – он показывает количество зарегистрированных событий тревоги, а также на изменившийся цвет значка компьютера SNS-Client в списке;



- щелкните на этом числовом индикаторе. Откроется панель "Журнал тревог", в которой вы увидите зарегистрированные события тревоги, полученные с компьютера SNS-Client;

Новый		СОБЫТИЯ		УГРОЗЫ				
			Дата	Событие	Категор...	Источник		Комп...
СТАНДАРТНЫЕ ЗАПРОСЫ			01.02.2022...	Учетной записи не удалось вы...	Logon	Microsoft...	SNS-Client	
За все время			01.02.2022...	Учетной записи не удалось вы...	Logon	Microsoft...	SNS-Client	
За час			01.02.2022...	Учетной записи не удалось вы...	Logon	Microsoft...	SNS-Client	
За сутки								
За 7 суток								
Все высокого уровня								
Все повышенного у...								
Все низкого уровня								
Последние 1000 соб...								

- переключитесь на вкладку "Угрозы" и убедитесь, что на основании зарегистрированных событий была сформирована одна угроза "Подбор пароля".

СОБЫТИЯ		УГРОЗЫ		
Угроза	Дата	Компьютер		
Подбор пароля	01.02.2022 23:57:...	SNS-Client.domain1.local		
Событие	Дата	Журнал	Категория	Источник
Учетной записи не у...	01.02.2022 23:57:26	Безопасно...	Logon	Microsoft-Windi
Учетной записи не у...	01.02.2022 23:57:32	Безопасно...	Logon	Microsoft-Windi
Учетной записи не у...	01.02.2022 23:57:38	Безопасно...	Logon	Microsoft-Windi

29. В панели "Компьютеры" выберите компьютер SNS-Client и в панели его свойств откройте вкладку "Информация". Просмотрите реквизиты в разделах "Уровень важности объекта" и "Учетная информация", которые могут использоваться администратором для идентификации данного компьютера при работе с системой Secret Net Studio.

Имя ▼

- Корневой
- domain1.local
 - ou_sns
 - SNS-Server.domain
 - SNS-Server.domain
 - SNS-Client.domain**
 - Admin-VM.domain
 - Domain Controllers

СОСТОЯНИЕ **НАСТРОЙКИ** **ИНФОРМАЦИЯ** **ЛИЦЕНЗИИ**

SNS-Client.domain1.local

Информация о клиенте Secret Net Studio

Домен(ы) безопасности: DOMAIN1.LOCAL\OU-SNS
 Тип: Агент Windows
 Версия Secret Net Studio: 8.8.15891.0
 Установленные обязательные пакеты исправлений: -
 Установленные пакеты исправлений: -

☐ Шифровать управляющий сетевой трафик
 Параметр будет доступен после настройки защищенного соединения на сервере.
 Подробнее смотрите в руководстве пользователя.

Уровень важности объекта ⓘ

Уровень важности объекта управления: ☒ Нормальный ☐ Высокий

Учетная информация

Название подразделения:

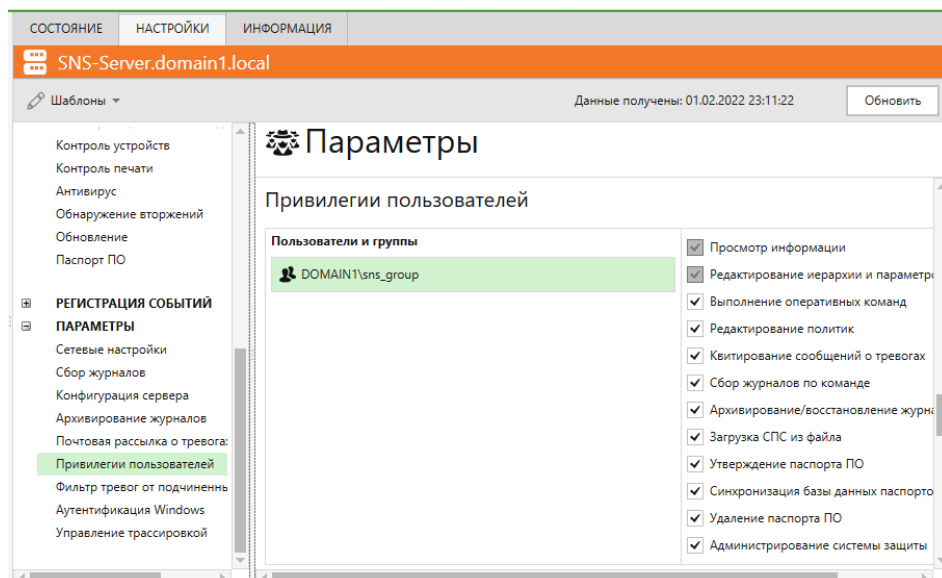
Название автоматизированной системы:

Обратите внимание, что можно изменить уровень важности объекта, который определяет присваиваемый уровень для событий тревоги, а также ввести данные о компьютере, которые будут использоваться при построении отчетов. Эти сведения могут редактироваться как централизованно, так и локально на защищаемом компьютере.

Установите для компьютера Admin-VM уровень важности "высокий" и примените изменения.

30. В панели "Компьютеры" выберите объект сервера безопасности и на вкладке "Настройки" откройте группу "Параметры / Привилегии пользователей". Данная группа доступна только при выборе СБ и предназначена для настройки привилегий пользователей для работы с программой управления.

С помощью кнопки ⓘ ознакомьтесь с кратким описанием привилегий.



Обратите внимание, что по умолчанию все перечисленные привилегии предоставлены пользователям, входящим в группу администраторов домена безопасности. При необходимости привилегии можно назначить и другим учетным записям, исключая привилегию "Редактирование иерархии и параметров объектов" – данная привилегия в обязательном порядке предоставляется только для группы администраторов домена безопасности.

31. Рассмотрен ряд важных операций по ведению журналов в Secret Net Studio. Останьтесь в текущем окне.

Выполнение сценария завершено.

Сценарий №5 "Управление подчинением защищаемых компьютеров серверу безопасности SNS"

В этом сценарии рассматриваются:

- внесение изменений в структуру оперативного управления на примере выведения (добавления) защищаемого компьютера из (в) подчинения серверу безопасности;
- возможность смены режима функционирования клиента – из автономного режима в сетевой и наоборот.

1. Рассмотрим внесение изменений в структуру оперативного управления. Перейдите в окно консоли VM Admin_VM. В панели "Компьютеры"

программы управления с помощью кнопки "Свойства" сверните панель свойств компьютера SNS-Client и нажмите кнопку "Структура ОУ"

Структура ОУ. В диаграмме оперативного управления содержатся выбранный сервер безопасности (с его подчиненными серверами, если они есть) и компьютеры, непосредственно подчиненные данному серверу.

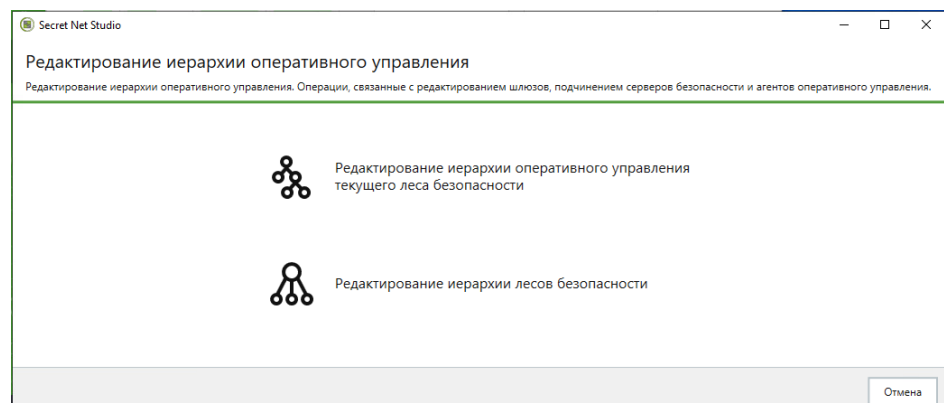
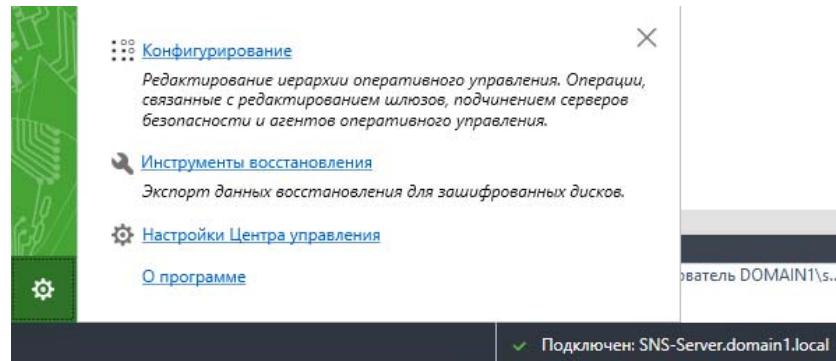
Имя	Высокий	Повышенный	Низкий	ФК	Сессии	Последнее	Лицензии	Домен
Корневой								
SNS-Server.domain1.local	1	6						DOMAIN1
SNS-Server.domain1.local		1		✓	DOMAIN1\snsa	Демо	Демо	DOMAIN1
SNS-Client.domain1.local		5		✓	DOMAIN1\snsa	Демо	Демо	DOMAIN1
Admin-VM.domain1.local	1			✓	DOMAIN1\snsa	Демо	Демо	DOMAIN1

Если при установке серверов безопасности и клиентов выполнялось их подчинение СБ, эти компьютеры будут включены в структуру оперативного управления (ОУ). Структура ОУ считается сформированной на достаточном уровне, если все защищаемые компьютеры присутствуют в ней и подчинены серверам безопасности.

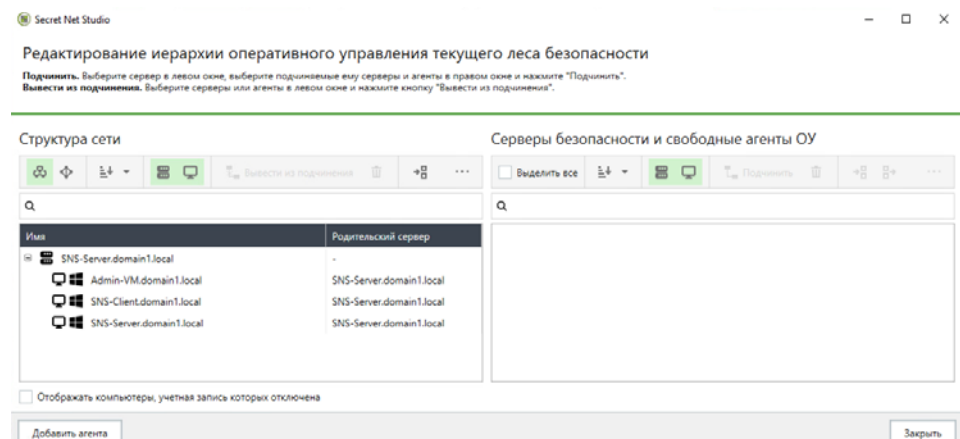
2. Изменения в структуре ОУ (добавление или исключение из нее защищаемых объектов) могут выполняться автоматически, при установке или удалении ПО системы Secret Net Studio на компьютерах. При необходимости в программе управления можно вручную вносить нужные изменения в сформированную структуру ОУ. Например, изменять отношения подчинения между серверами безопасности или подчинять защищаемые компьютеры другим СБ. Переподчинение объектов (например, при пересмотре сетевой структуры) требует предварительного вывода их из подчинения текущим СБ.

В качестве примера проведения изменений в структуре ОУ выведите компьютер SNS-Client из подчинения серверу SNS-Server. Для этого:

- в нижней части панели навигации (слева в основном окне) нажмите кнопку "Настройки"  и в открывшейся панели нажмите кнопку-ссылку "Конфигурирование". На экране появится диалоговое окно выбора режима редактирования;

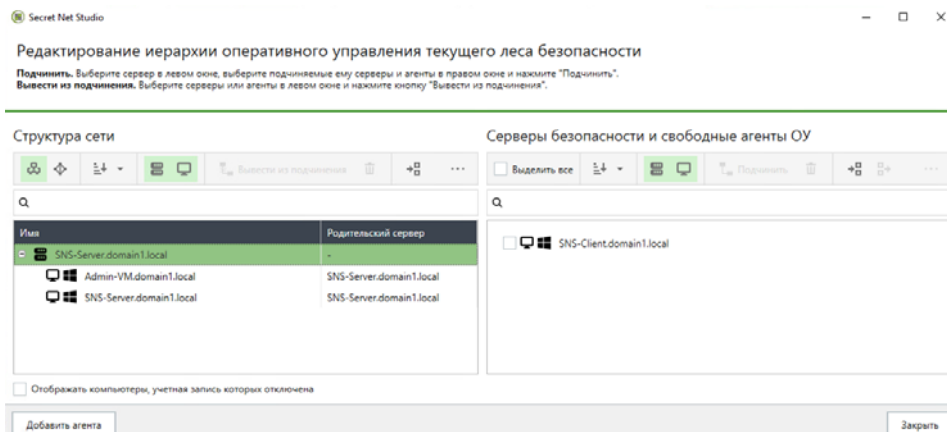


- поскольку в данном задании изменяется структура ОУ текущего леса безопасности, выберите вариант  "Редактирование иерархии оперативного управления...". Откроется окно, в левой части которого представлена текущая структура объектов управления, а в правой – список защищаемых компьютеров и серверов безопасности, доступных для подчинения выбранному серверу;



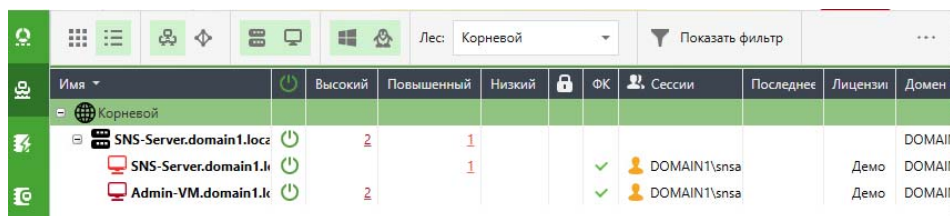
Обратите внимание, что при необходимости с помощью кнопок и текстового поля для поиска, расположенных над списками объектов, а также переключателя "Отображать компьютеры, учетная запись которых отключена" можно фильтровать списки объектов по типу, контексту или по состоянию учетной записи.

- в левом списке "Структура сети", в структуре сервера безопасности выберите компьютер SNS-Client и нажмите кнопку "Вывести выбранные объекты из подчинения"  **Вывести из подчинения**. В появившемся диалоговом окне запроса подтвердите выполнение операции. Выбранный объект перестанет отображаться в списке "Структура сети" и будет перемещен в список свободных агентов относительно выбранного СБ.



Примечание. При выводе объекта из подчинения текущему СБ этот объект становится свободным. Свободный компьютер в дальнейшем необходимо подчинить СБ. Если из подчинения выведен сервер безопасности, то он может продолжать функционировать в качестве независимого объекта управления.

3. Закройте диалоговое окно "Редактирование иерархии оперативного управления" и вернитесь в программу управления к диаграмме управления в режиме отображения списков компьютеров. Обратите внимание, что выведенный из подчинения компьютер не представлен в структуре ОУ после обновления ее конфигурации.



4. В нижней части панели навигации (слева в основном окне) нажмите кнопку "Настройки"  и, используя описание пп. 2, 3, восстановите подчинение компьютера SNS-Client серверу SNS-Server и убедитесь, что подчиненный компьютер появился в диаграмме управления.

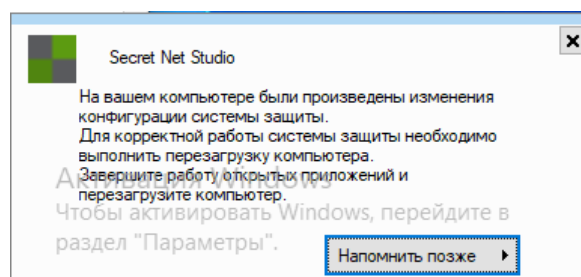
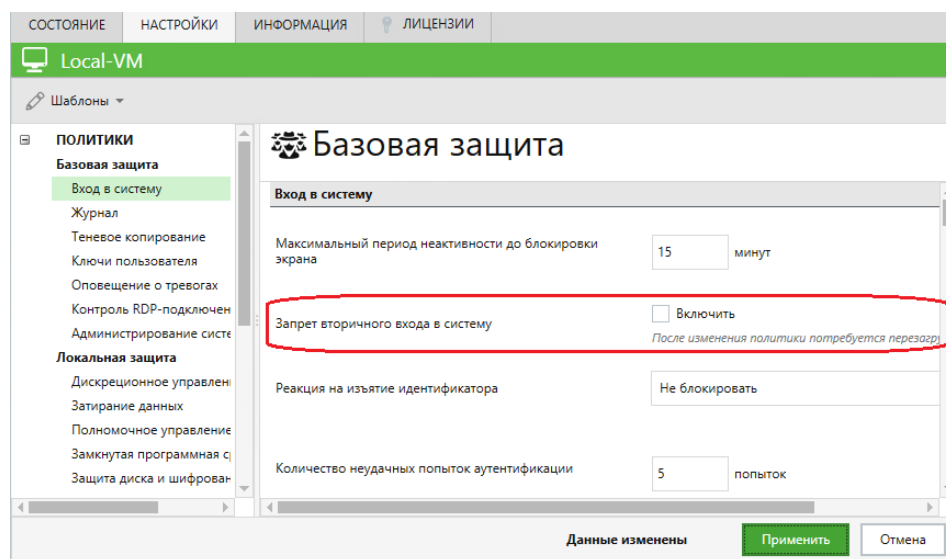
Примечание. В реальной работе можно добавить в качестве объекта структуры ОУ любой компьютер, зарегистрированный в Active Directory. Если домен безопасности сформирован на базе вложенного контейнера Active Directory (в организационном подразделении), перед добавлением в структуру ОУ компьютеры следует переместить в этот контейнер, используя штатные средства администрирования AD.

Включение в домен компьютеров под управлением ОС семейства Linux с установленным СЗИ Secret Net LSP осуществляется отдельно при настройке удаленного управления (см. соответствующее описание последовательности действий в руководстве администратора по Secret Net LSP).

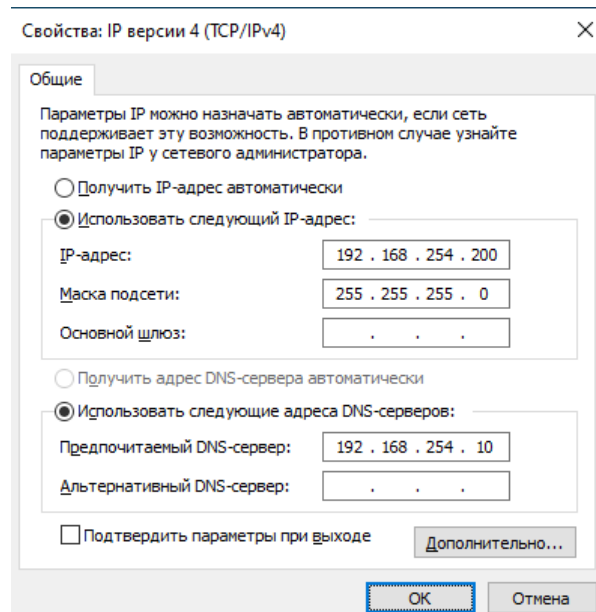
5. Далее показывается возможность смены режима функционирования клиента Secret Net Studio из автономного в сетевой и обратно на примере компьютера Local-VM. Данная операция доступна только в локальном режиме работы программы управления.

Перед изменением режима работы клиента на компьютере Local-VM проведите необходимые настройки:

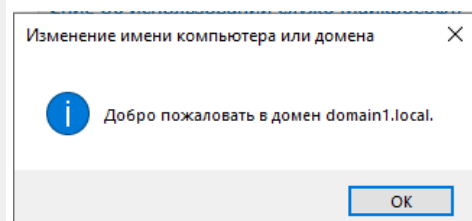
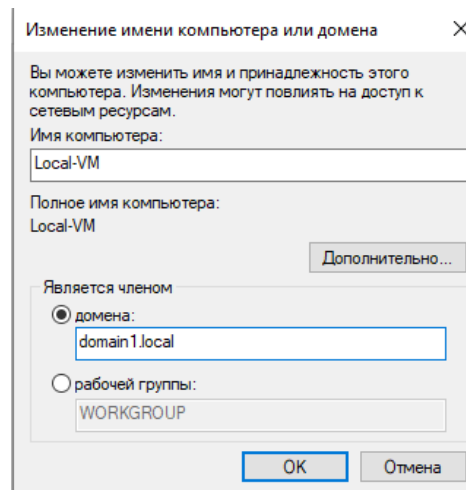
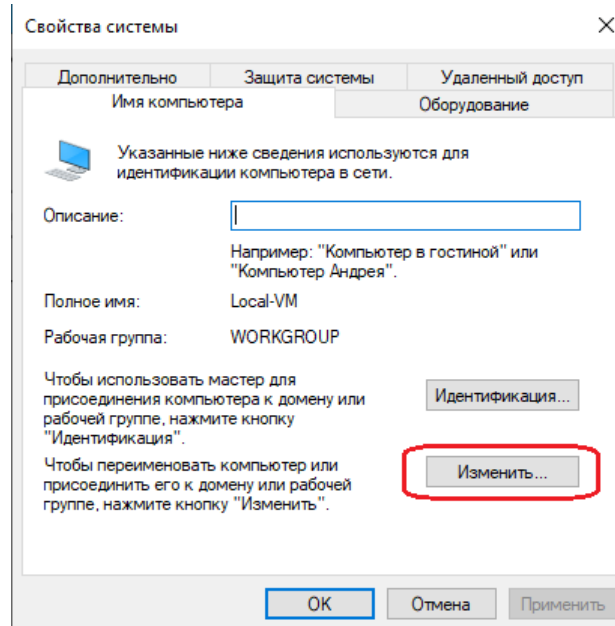
- откройте окно консоли VM Local_VM и в программе управления, в группе настроек "Политики / Базовая защита / Вход в систему" отключите параметр "Запрет вторичного входа в систему", а затем нажмите кнопку "Применить". В области уведомлений рабочего стола Windows обратите внимание на появившееся сообщение о необходимости перезагрузки;



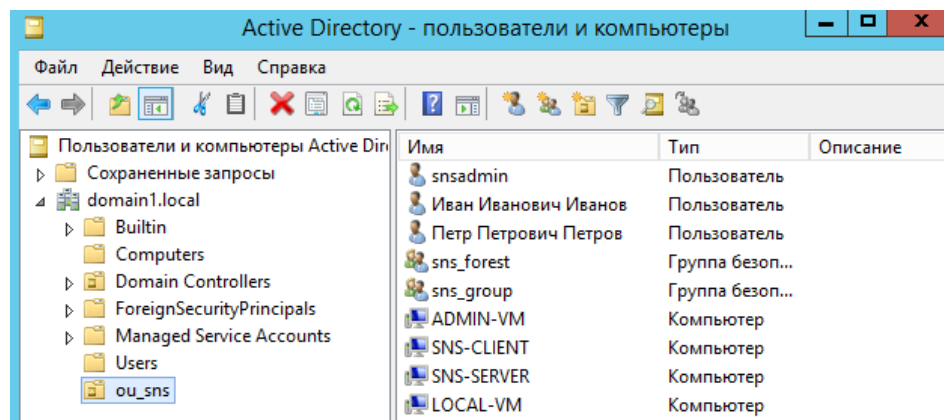
- чтобы изменения вступили в силу, перезагрузите VM Local_VM и авторизуйтесь под учетной записью **admin / P@ssw0rd**;
- установите следующие параметры сетевого адаптера:
 - отключите протокол IPv6;
 - "IP-адрес" – **192.168.254.200**;
 - "Маска подсети" – **255.255.255.0**;
 - "Предпочитаемый DNS-сервер" – **192.168.254.10**;



- введите компьютер Local-VM в домен **domain1.local**, указав реквизиты администратора домена **Администратор /P@ssw0rd**. Перезагрузите ОС и авторизуйтесь под учетной записью администратора домена;

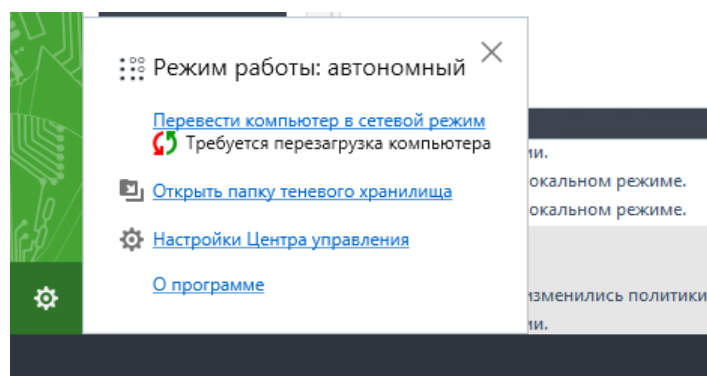


- на компьютере Local-VM добавьте доменную группу "sns_group" в группу локальных администраторов, а затем переавторизуйтесь под учетной записью администратора домена безопасности "snsadmin";
- переключитесь в окно консоли контроллера домена DC, откройте оснастку "Active Directory – Пользователи и компьютеры" и переместите компьютер Local-VM в подразделение "ou_sns".

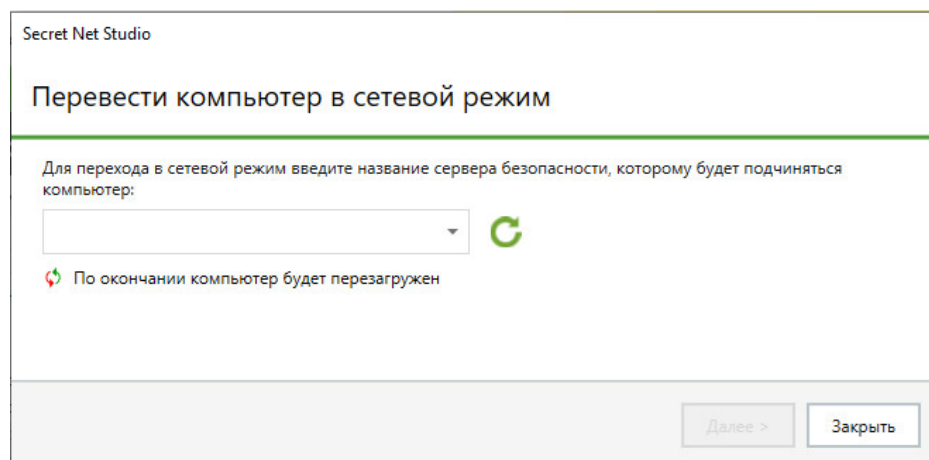


6. Измените на компьютере Local-VM режим функционирования клиента Secret Net Studio из автономного в сетевой. Для этого:

- запустите локальный центр управления и откройте панель "Настройки" . Обратите внимание, что в открывшейся панели указан текущий режим работы – "автономный";

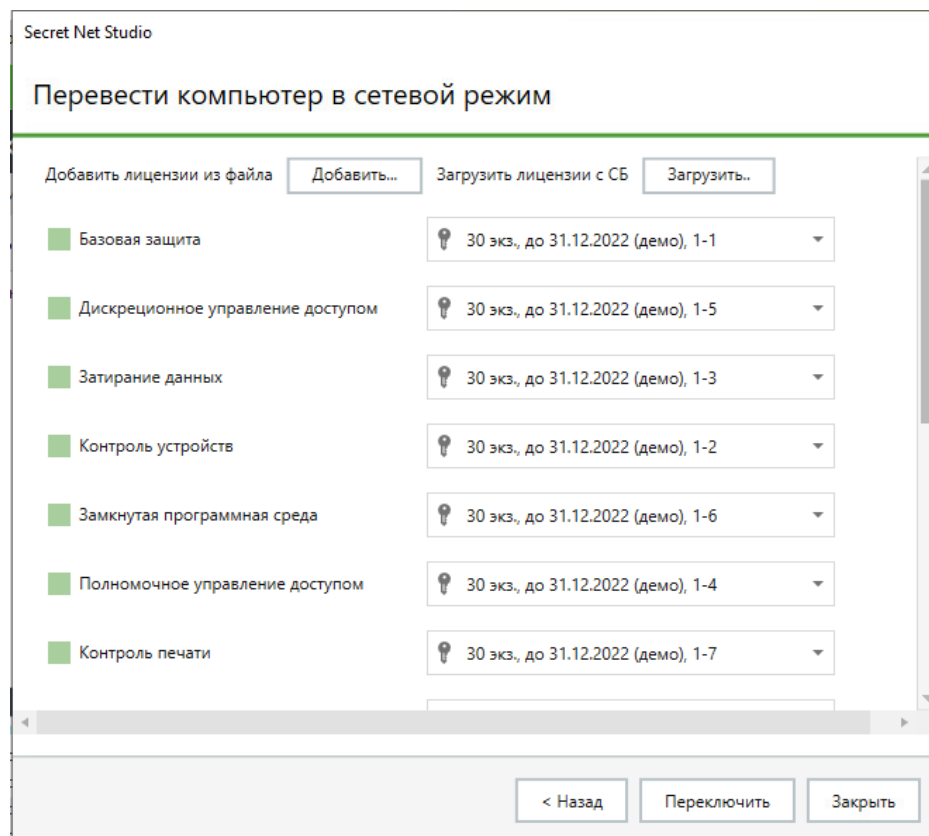


- нажмите кнопку-ссылку "Перевести компьютер в сетевой режим". Откроется окно перехода в сетевой режим и поиска СБ;

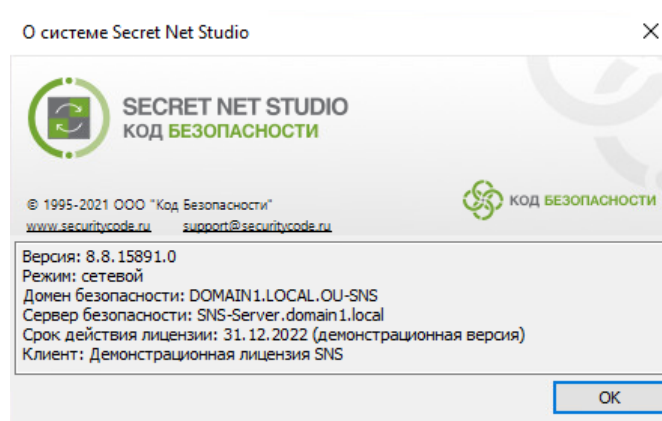


- справа от поля ввода названия сервера нажмите кнопку "Поиск сервера безопасности" и после появления в данном поле имени "SNS-Server.domain1.local" нажмите кнопку "Далее";

- в открывшемся окне перевода компьютера в сетевой режим проверьте добавление всех необходимых лицензий и при необходимости добавьте недостающие (не активируйте компонент "Доверенная среда", поскольку его нельзя использовать в виртуальной среде);

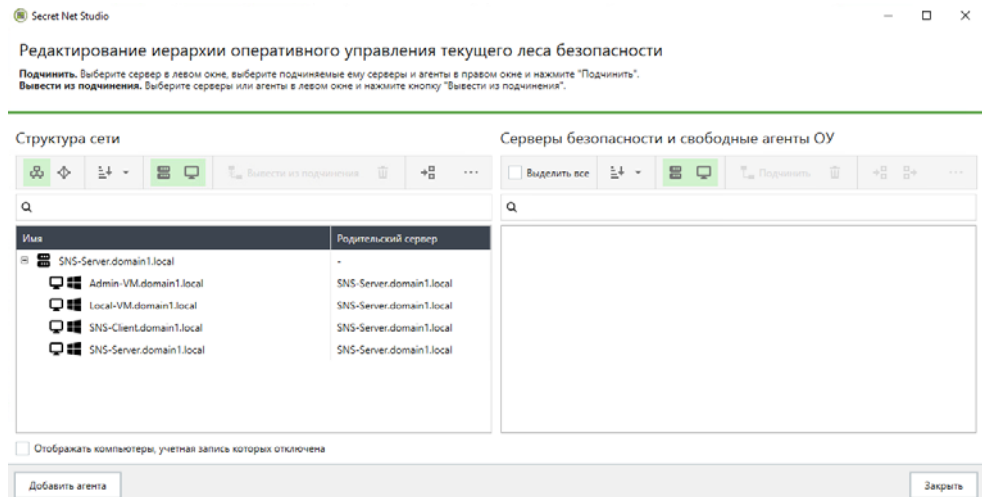


- нажмите кнопку "Переключить" и дождитесь завершения настройки компьютера для работы в сетевом режиме. Перезагрузите ОС и авторизуйтесь под учетной записью "snsadmin". Теперь на VM Local_VM клиент Secret Net Studio работает в сетевом режиме. Убедитесь в этом – в области трея Windows раскройте контекстное меню значка Secret Net Studio, выберите опцию "О системе", ознакомьтесь с представленной информацией, а затем закройте окно.

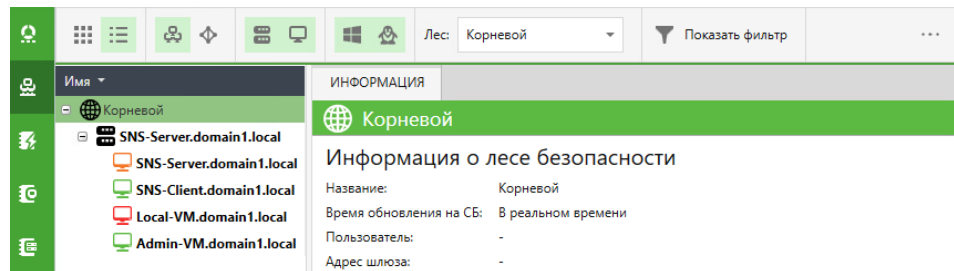


7. Убедитесь, что значок компьютера Local-VM появился в структуре оперативного управления СБ SNS-Server. Для этого:
 - переключитесь в окно VM Admin_VM, в окне программы управления в нижней части панели навигации (слева в основном окне) нажмите кнопку "Настройки"  и в открывшейся панели нажмите кнопку-ссылку "Конфигурирование". Далее выберите режим редактирования иерархии оперативного управления текущего леса безопасности, в диалоговом окне "Редактирование иерархии оперативного управления..." разверните

структуру объекта сервера безопасности и убедитесь, что в нее добавлен компьютер Local-VM;



- закройте диалоговое окно "Редактирование иерархии оперативного управления..." и убедитесь, что компьютер Local-VM присутствует в структуре оперативного управления панели "Компьютеры" .



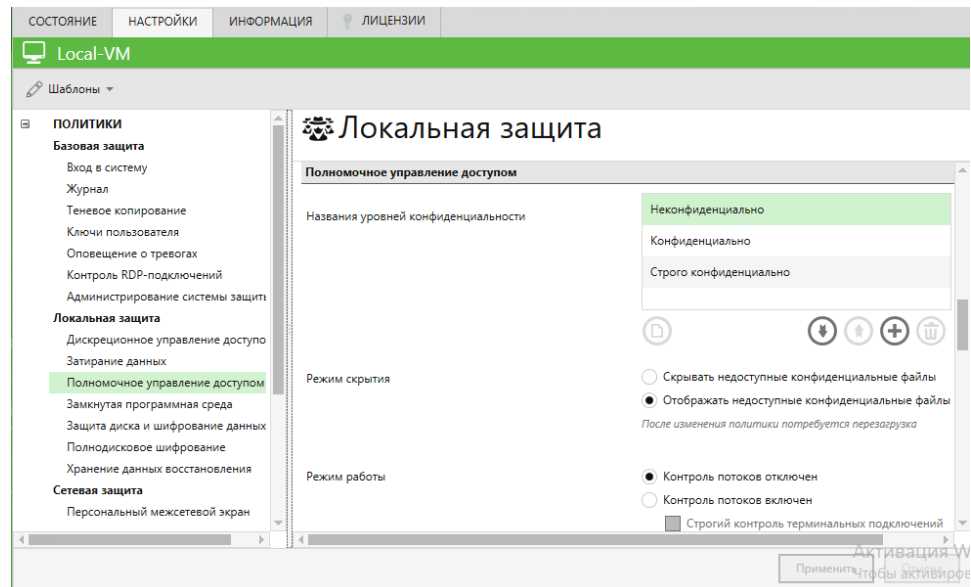
Теперь для данного компьютера будут действовать централизованно заданные администратором безопасности настройки и политики защиты Secret Net Studio.

8. Самостоятельно. Выведите компьютер Local-VM из подчинения серверу безопасности: последовательно переключите сетевой режим работы клиента SNS обратно в автономный (см. п. 6), в оснастке "Active Directory – Пользователи и компьютеры" переместите в папку "Computers" компьютер Local-VM (см. п. 5) и выведите его из домена domain1.local, а затем отключите на нем сетевой интерфейс (см. п. 5). Убедитесь, что компьютер Local-VM больше не отображается в структуре оперативного управления (см. п. 7).
9. Рассмотрены возможности управления подчинением защищаемых компьютеров серверу безопасности SNS. Оставайтесь в текущем окне.
Выполнение сценария завершено.

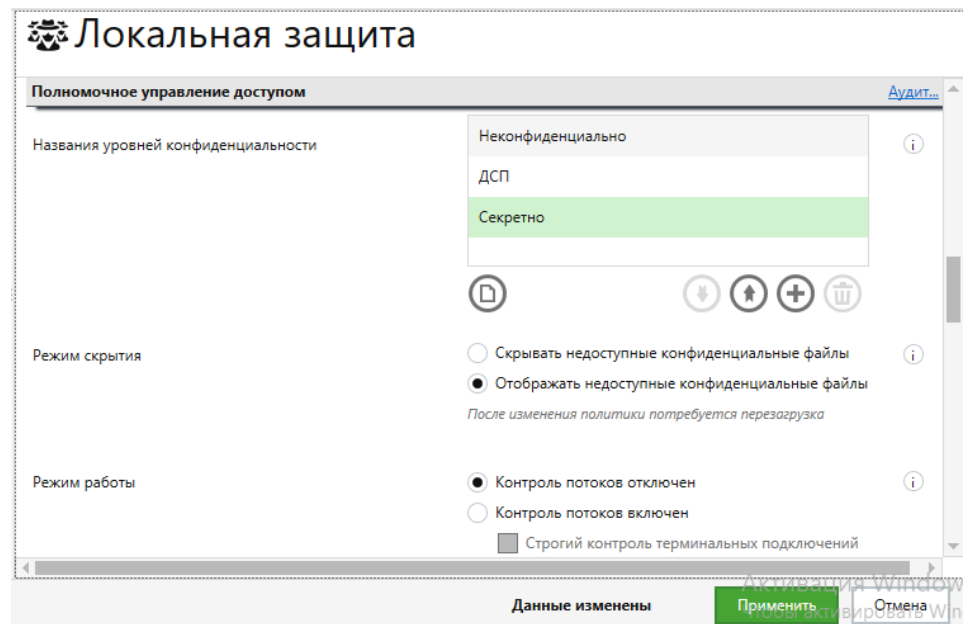
Сценарий №6 "Настройка полномочного управления доступом"

В данном сценарии иллюстрируется выполнение системой защиты проверки соответствия уровня допуска пользователя и категории конфиденциальности объекта доступа (каталога или файла).

1. Откройте консоль VM Local_VM и убедитесь, что вход в систему выполнен с учетной записью "admin". Запустите "Локальный центр управления" и раскройте панель "Компьютер" .
2. Для первоначальной настройки механизма полномочного управления доступом определите следующие категории конфиденциальности: "неконфиденциально", "ДСП" (для служебного пользования), "секретно". Для этого выполните следующие действия:
 - в ПУ выберите вкладку "Настройки" и раскройте группу "Политики / Локальная защита / Полномочное управление доступом";



- используя расположенные справа кнопки , ознакомьтесь с информацией об имеющихся настройках данной защитной подсистемы. Обратите внимание, что заданные по умолчанию первые три уровня конфиденциальности можно только переименовать;
- в поле "Названия уровней конфиденциальности" выберите значение "Конфиденциально" и с помощью клавиши [F2] переименуйте его в "ДСП" (вместо клавиши [F2] можно использовать двойной щелчок);
- аналогично переименуйте название "Строго конфиденциально" в "Секретно";
- в поле "Режим скрытия" оставьте заданную по умолчанию опцию "Отображать недоступные конфиденциальные файлы";
- убедитесь, что в поле "Режим работы" по умолчанию выбрана опция "Контроль потоков отключен";

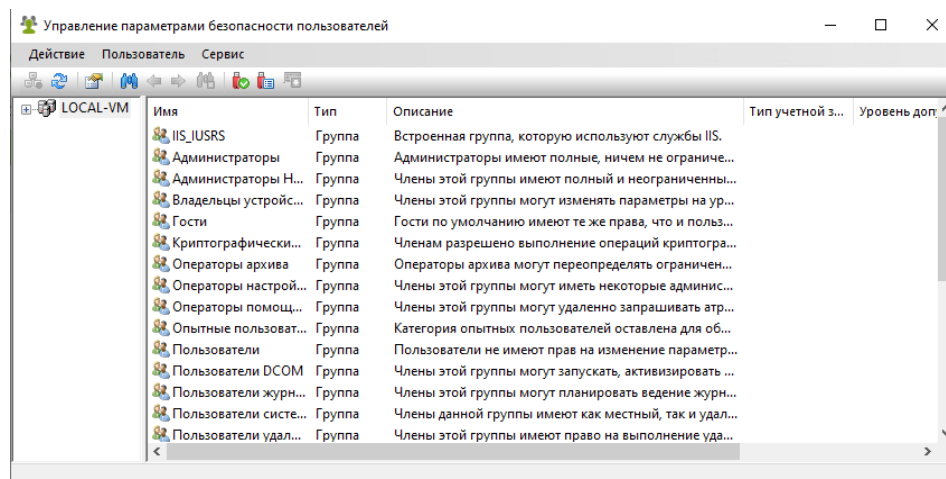


- нажмите кнопку "Применить" и просмотрите появившуюся запись в панели событий системы.

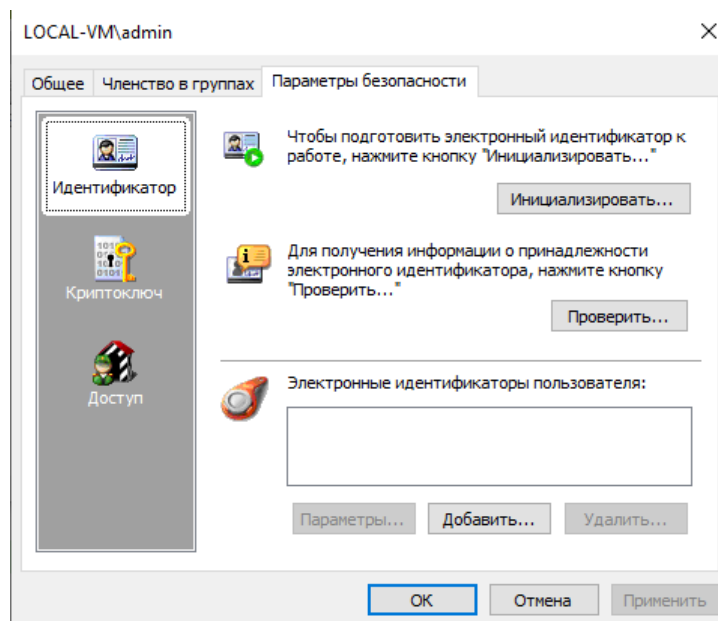
Примечание. Обратите внимание на переключатели "Скрывать / Отображать недоступные конфиденциальные файлы". После включения режима скрытия пользователю в различных файловых менеджерах не будут показываться имена конфиденциальных файлов, доступ к которым ему запрещен. При этом:

- если контроль потоков отключен, пользователь не будет видеть файлы, категория конфиденциальности которых выше его уровня допуска;
- если контроль потоков включен, пользователь, независимо от его уровня допуска, не увидит файлы, категория конфиденциальности которых выше уровня конфиденциальности текущей сессии;
- имена каталогов любой категории конфиденциальности отображаются всегда.

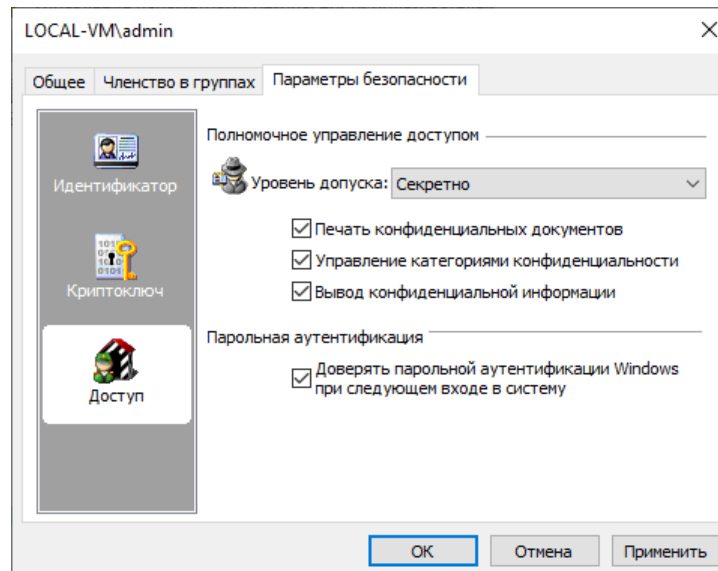
3. Назначьте уровни допуска и привилегии пользователей на компьютере Local-VM. Для этого запустите программу "Управление пользователями": "Пуск / Код Безопасности / Управление пользователями" и выполните следующие действия:



- откройте окно свойств учетной записи администратора "admin" и выберите вкладку "Параметры безопасности";

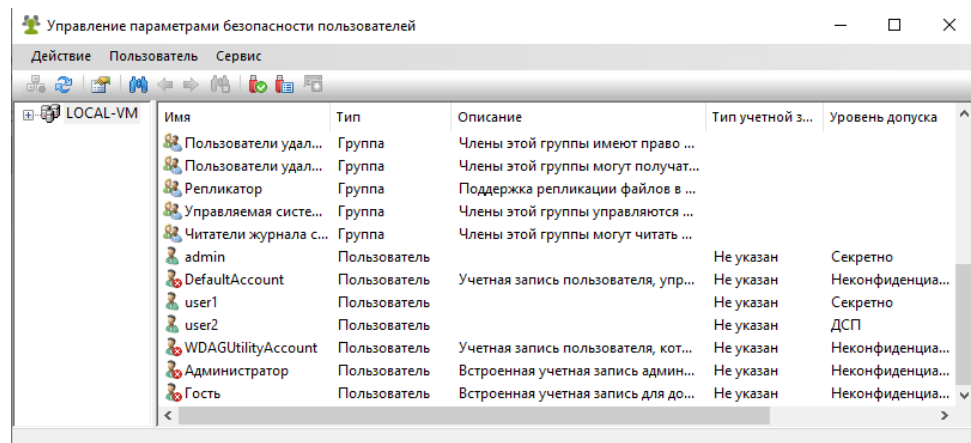


- выберите категорию настроек "Доступ", установите самый высокий уровень допуска "Секретно" и включите все привилегии;

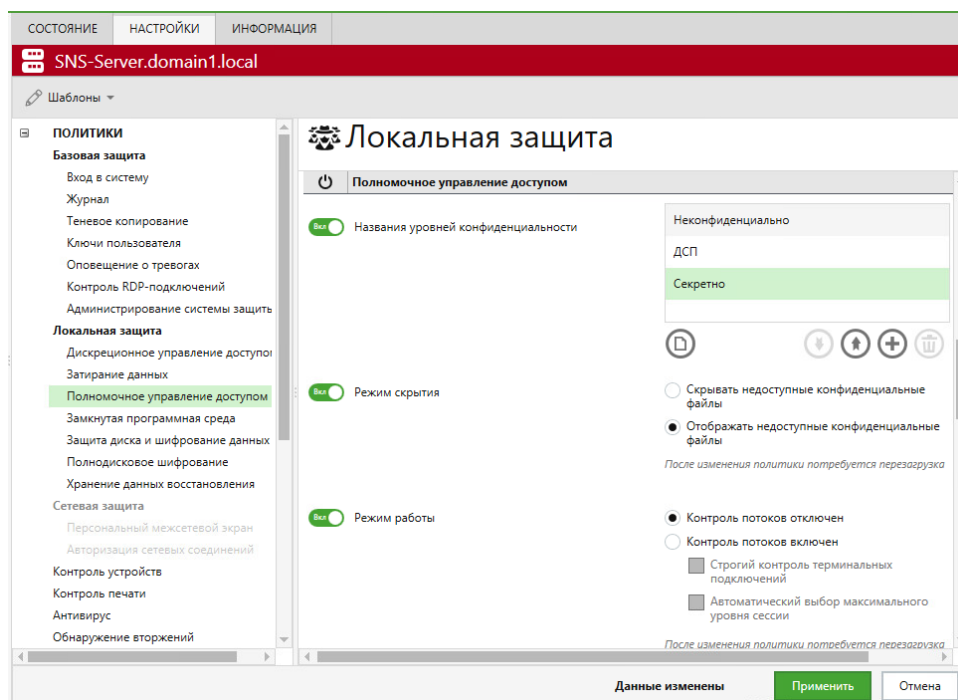


- нажмите кнопку "ОК". Аналогично для пользователей "user1" и "user2" назначьте следующие уровни доступа и установите все привилегии:
 - user1 (Иван Иванович Иванов) – Секретно;
 - user2 (Петр Петрович Петров) – ДСП.

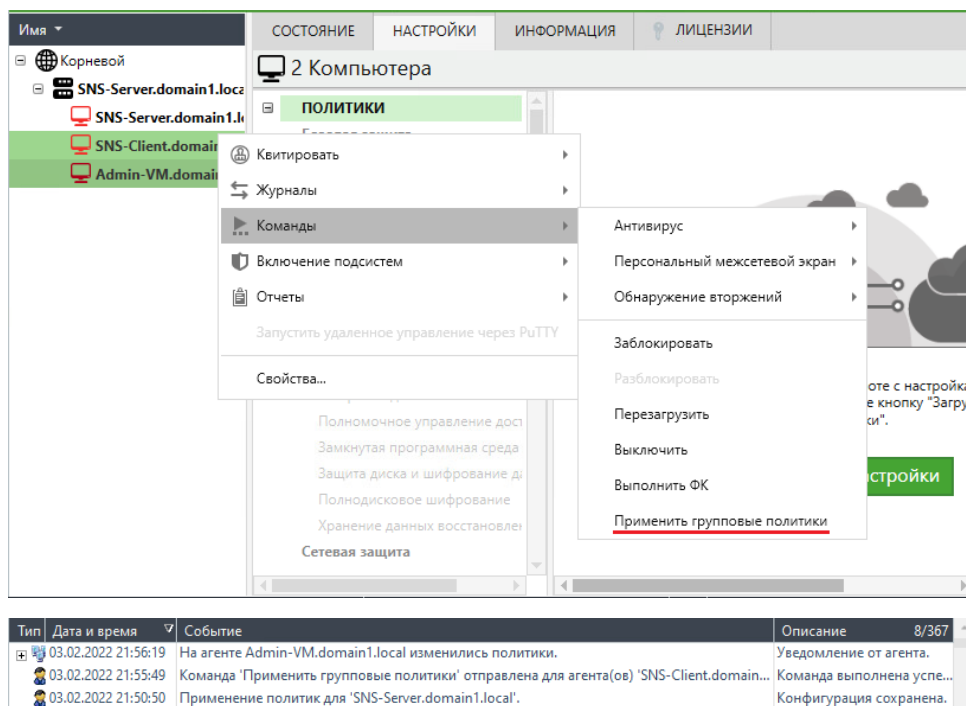
Примечание. Назначенные уровни допуска и привилегии вступают в силу при следующем входе пользователя в систему.



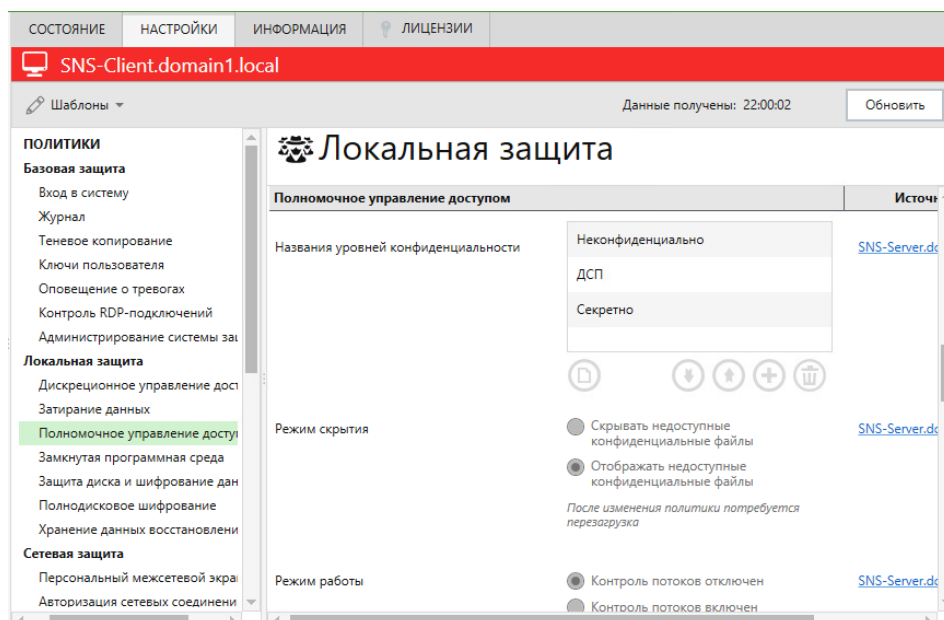
4. Используя описание пп. 1–2, на VM Admin_VM под учетной записью "snsadmin" выполните аналогичную первоначальную настройку механизма полномочного управления доступом в сетевом варианте для групповых политик сервера подключения SNS-Server.



5. Сохраните сделанные изменения. Для компьютеров SNS-Client и Admin_VM с помощью опции контекстного меню "Команды / Применить групповые политики" принудительно примените измененные групповые политики. Обратите внимание на сообщения в панели событий об успешном применении групповых политик.

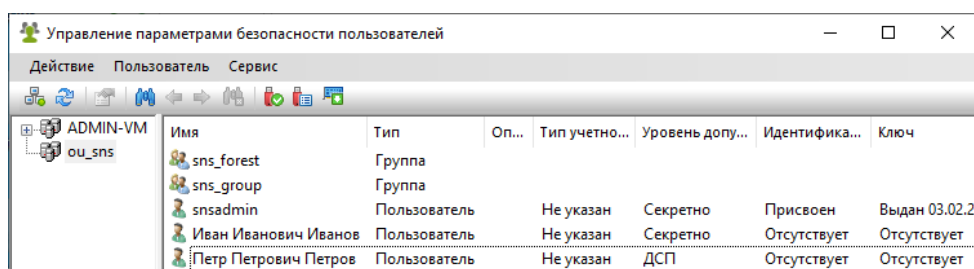


6. Убедитесь, что настроенные групповые политики уровней полномочного управления доступом теперь действуют на защищаемых компьютерах SNS-Client и Admin-VM. Для этого последовательно просмотрите настройки группы политик "Политики / Локальная защита / Полномочное управление доступом" каждого из этих компьютеров.

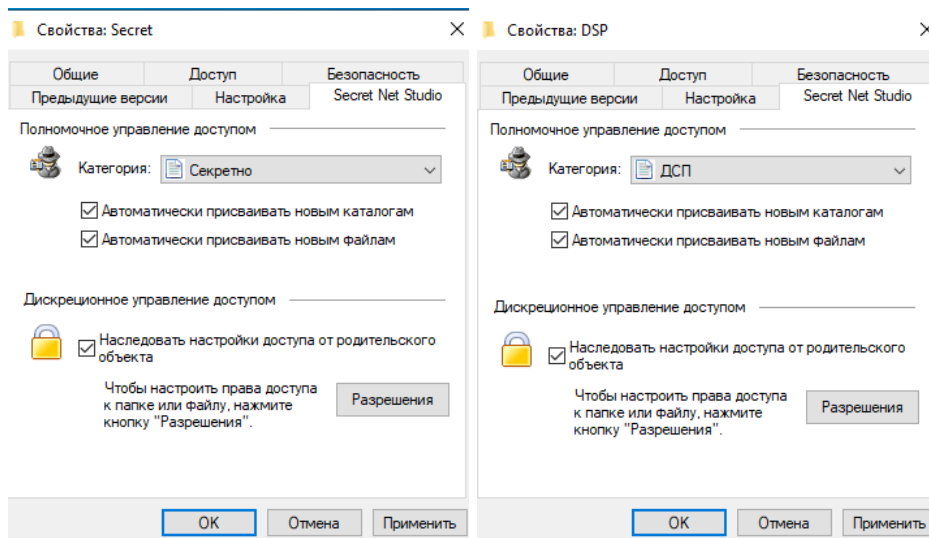


7. Используя описание п. 3, на VM Admin_VM выполните аналогичную настройку уровней доступа и привилегий в сетевом варианте программы "Управление пользователями" для доменных пользователей:

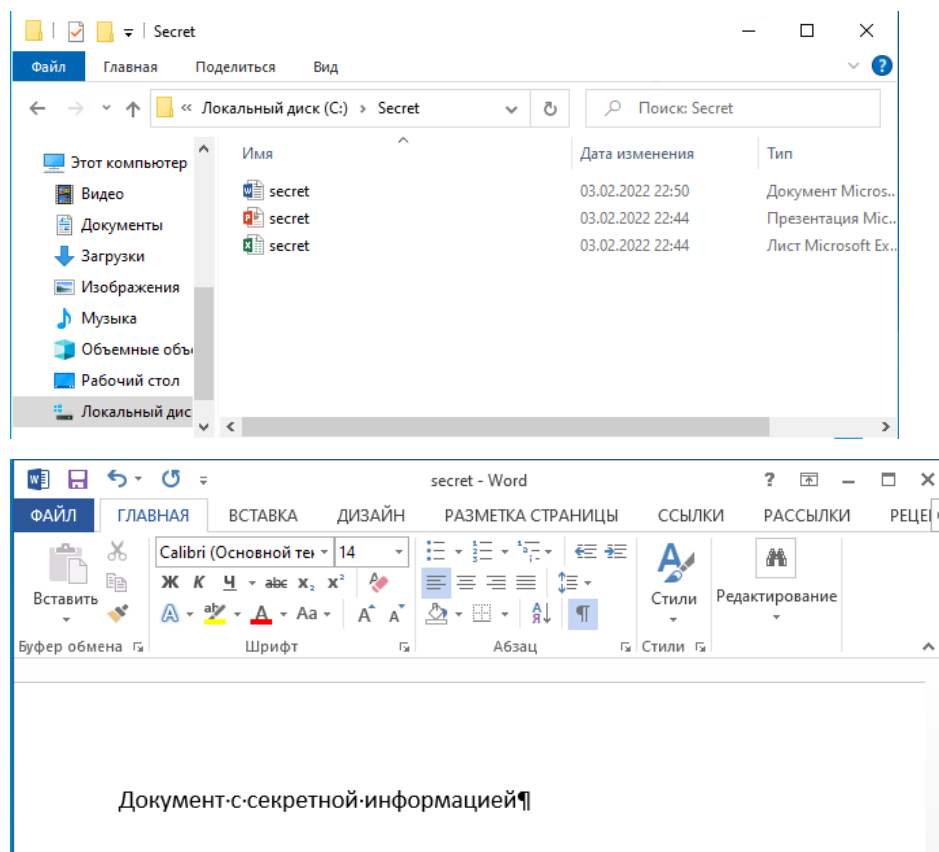
- snsadmin – Секретно;
- user1 (Иван Иванович Иванов) – Секретно;
- user2 (Петр Петрович Петров) – ДСП.



8. В консоли VM Local_VM переавторизуйтесь под учетной записью "admin", чтобы назначенный ранее уровень допуска и привилегии вступили в силу. Создайте на диске "C:" папки "Secret", "DSP" и "Not_conf" и назначьте для каждой из них в соответствии с названием категорию конфиденциальности.



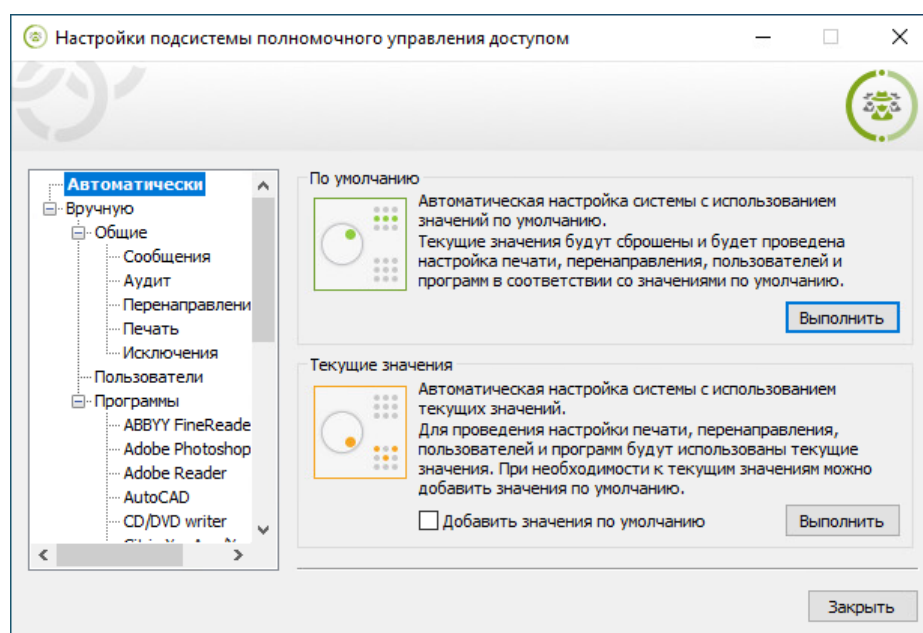
9. В папке "C:\Secret" создайте документы форматов Microsoft Word, Microsoft PowerPoint и Microsoft Excel с произвольным содержанием: "secret.docx", "secret.pptx" и "secret.xlsx" соответственно.



10. Аналогично – в папке "C:\DSP" создайте документы "dsp.docx", "dsp.pptx" и "dsp.xlsx".

11. Чтобы обеспечить функционирование механизма полномочного управления доступом при включенном режиме контроля потоков, проведите дополнительную настройку локально на компьютере. Подобная настройка должна выполняться перед включением режима контроля потоков, а также в процессе эксплуатации системы при добавлении новых пользователей, программ, принтеров для оптимизации функционирования механизма.

В окне VM Local_VM загрузите программу настройки подсистемы полномочного управления доступом: "Пуск / Код Безопасности / Программа настройки подсистемы полномочного управления доступом".



12. В программе "Настройка подсистемы полномочного управления доступом" реализованы средства как для автоматической настройки, так и для конфи-

гуирования вручную. При автоматической настройке выполняется базовый набор действий, после которых обеспечивается функционирование механизма и совместимость со стандартным и наиболее распространенным программным обеспечением.

Автоматическая настройка со значениями по умолчанию применяется в случае необходимости удалить текущую конфигурацию и вернуть исходные значения параметров. Это может потребоваться, если значения параметров некорректно заданы или удалены, а также при первичной настройке системы с минимально необходимой конфигурацией для функционирования механизма в режиме контроля потоков.

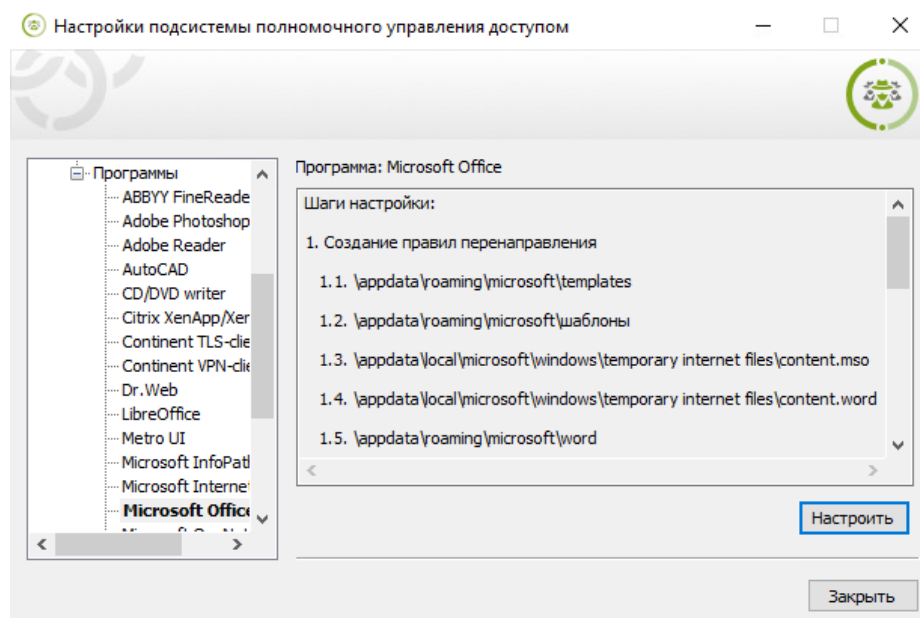
Вариант настройки "Текущие значения" предназначен для повторного применения в системе заданных значений параметров. Это позволяет восстановить настройку системы при сбоях функционирования механизма или при добавлении в систему новых пользователей, программ, принтеров и других объектов, задействованных в механизме полномочного управления доступом и контроля печати. При такой настройке дополнительно к текущим значениям параметров можно добавить исходные значения (значения по умолчанию). При этом текущие значения не удаляются.

Ручная настройка предусмотрена для выполнения специфических действий, например, для обеспечения совместной работы с ПО, которое не входит в список для автоматической настройки. Можно вручную изменять параметры работы механизма полномочного управления доступом и контроля печати, что позволяет обеспечить функционирование с учетом особенностей программной среды компьютера и предпочтений пользователя.

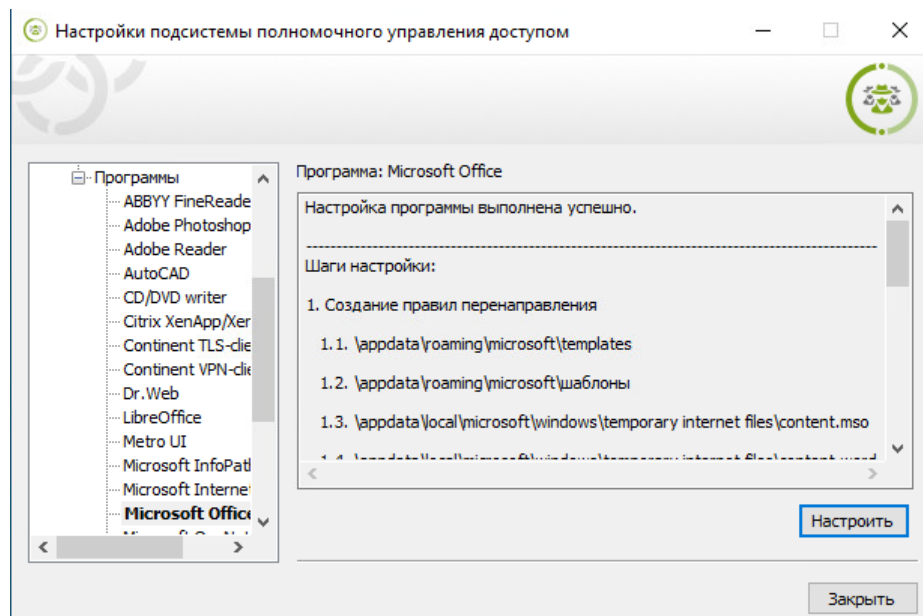
Средства для ручной настройки параметров представлены в следующих основных разделах:

- "Общие" – для настройки общих параметров работы пользователей и приложений;
- "Пользователи" – для настройки параметров, относящихся к профилям пользователей;
- "Программы" – для настройки параметров для приложений.

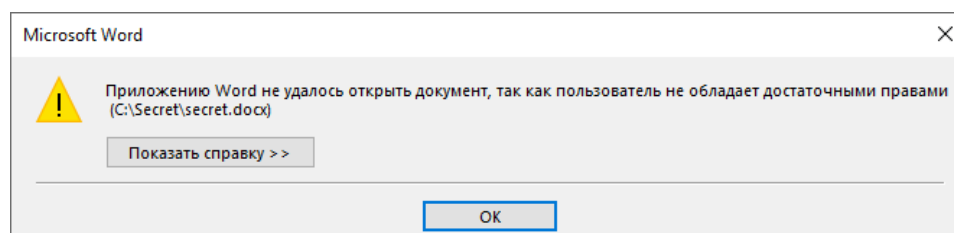
Запустите настройку для программ Microsoft Office. Для этого в разделе настроек выберите "Вручную / Программы / Microsoft Office" и нажмите кнопку "Настроить".



13. Программа проведет настройку перенаправления файлов. Дождитесь завершения этого процесса. После создания правил перенаправления появится окно с информацией об успешном проведении настройки.



14. Закройте окно "Настройка подсистемы полномочного управления доступом". На VM Local_VM перезагрузите ОС и авторизуйтесь под учетной записью "user2 (Петров Петр Петрович)" с уровнем допуска "ДСП".
15. Сделайте попытку открытия любого файла из папки "C:\Secret". Поскольку уровень допуска пользователя "user2" ниже, чем уровень конфиденциальности данного каталога и его содержимого, механизм полномочного управления доступом Secret Net Studio не позволит открыть документ, и система выдаст соответствующее сообщение.



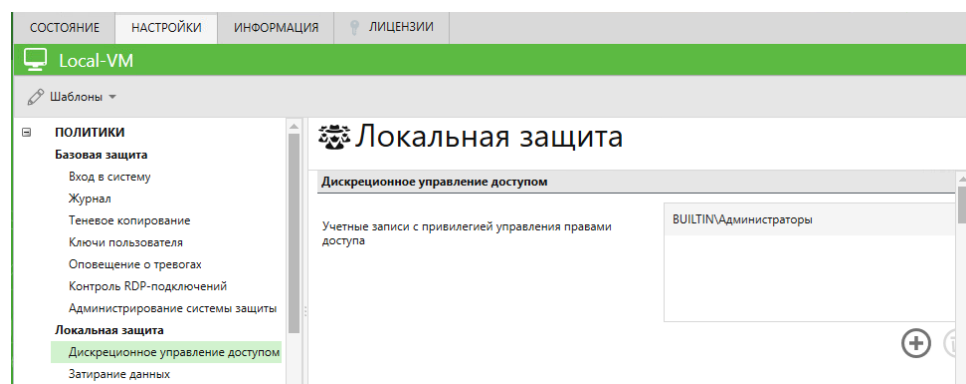
16. Переавторизуйтесь на VM Local_VM под учетной записью пользователя "user1 (Иванов Иван Иванович)", сделайте аналогичную попытку открытия любого файла из папки "C:\Secret" и сравните результат.
17. Проведите проверку работы полномочного управления доступом в сетевом варианте. Для этого:
 - переавторизуйтесь на VM SNS-Server под учетной записью "snsadmin" и создайте на диске "C:" общедоступную папку "user_files" с максимальными разрешениями (permissions) на уровне ОС Windows;
 - в папке "user_files" создайте подпапки "Secret" и "DSP". Используя описание пп. 8–10, установите для них соответствующий уровень допуска и создайте в них файлы формата .rtf с произвольным содержанием;
 - на VM SNS_Client и Admin_VM последовательно переавторизуйтесь под учетной записью "snsadmin" и, используя описание пп. 11–14, проведите на них локально настройку полномочного управления доступом;
 - на VM SNS_Client последовательно переавторизуйтесь под доменными учетными записями "user2" и "user1", попробуйте открыть с помощью Microsoft Word файлы из общедоступных папок "user_files\Secret" и "user_files\DSP" с компьютера SNS-Server и сравните результат.

Выполнение сценария завершено.

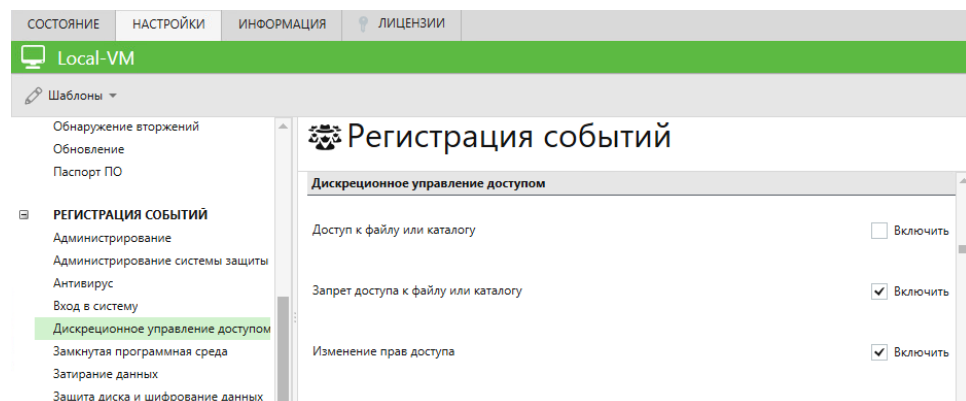
Сценарий №7 "Настройка механизма дискреционного управления доступом"

В этом сценарии тестируется работа механизма дискреционного управления доступом на примере текстовых файлов.

1. На VM Local_VM переавторизуйтесь под учетной записью администратора "admin".
2. На диске "C:" создайте следующие защищаемые ресурсы:
 - папку "Ivanov" и в ней файл произвольного содержания "document.txt";
 - папку "Petrov" и в ней файл произвольного содержания "graph.txt";
 - папку "Common" и в ней файл произвольного содержания "plan.txt".
3. Убедитесь, что администратору предоставлены привилегии для изменения прав доступа на любых ресурсах, а также настроена регистрация событий, связанных с доступом к ресурсам. Для этого:
 - запустите программу "Локальный центр управления", в панели "Компьютер"  выберите вкладку "Настройки" и откройте группу политик "Политики / Локальная защита / Дискреционное управление доступом";



- убедитесь, что в поле "Учетные записи с привилегией управления правами доступа" выбрана по умолчанию группа локальных администраторов, и с помощью расположенной справа кнопки  ознакомьтесь с описанием этой настройки. Обратите внимание, что при необходимости, используя кнопку "Добавить" , можно установить привилегию управления правами доступа для ресурсов другому пользователю или группе пользователей;
- справа от названия группы "Дискреционное управление доступом" нажмите кнопку-ссылку "Аудит..." и переключитесь в раздел настроек "Регистрация событий / Дискреционное управление доступом";



- с помощью расположенной справа от настроек кнопки  ознакомьтесь с описанием событий. Обратите внимание, что в целях минимизации размера журнала событий факт доступа к файлу или каталогу по умолчанию не регистрируется.

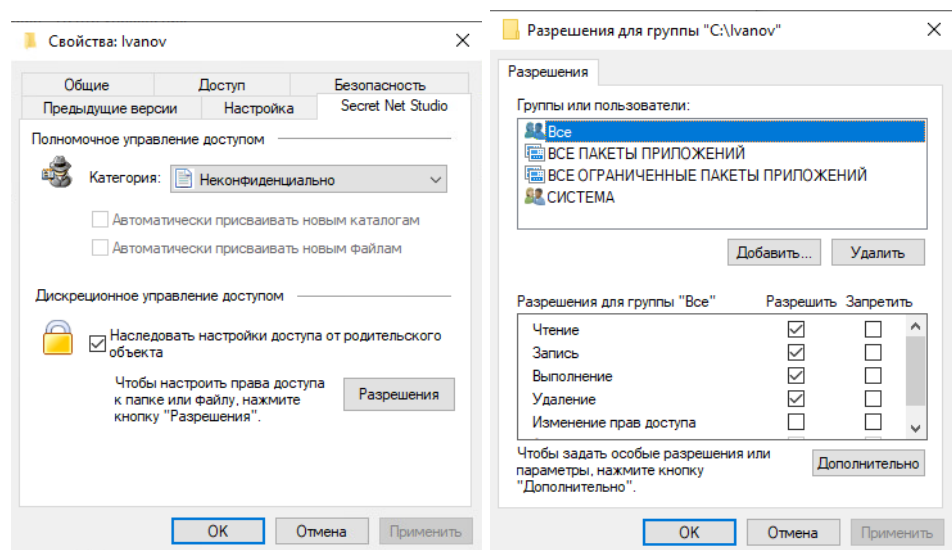
4. Установите права дискреционного доступа для пользователей "user1 (Иванов Иван Иванович)" и "user2 (Петров Петр Петрович)" в соответствии с матрицей доступа, приведенной в таблице.

Пользователи	Документы		
	C:\Ivanov\document.txt	C:\Petrov\graph.txt	C:\Common\plan.txt
user1 (Иванов Иван Иванович)	rx	r	Все разрешения
user2 (Петров Петр Петрович)	-	rwX	r

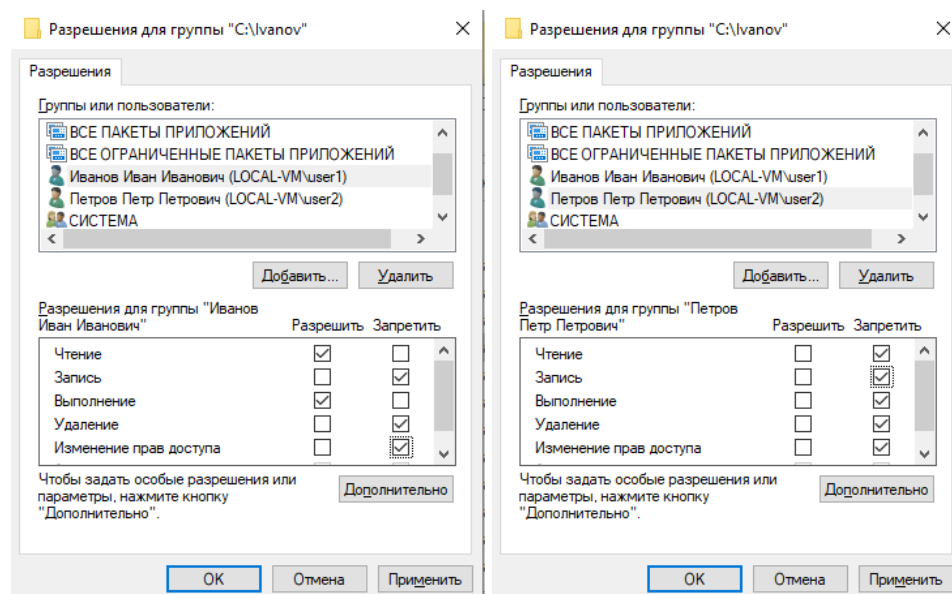
Где r – чтение, w – запись/изменение, d – удаление, x – выполнение.

Для установки прав дискреционного доступа для папки "C:\Ivanov" сделайте следующее:

- через контекстное меню данной папки откройте диалоговое окно "Свойства" и выберите вкладку "Secret Net Studio". В разделе "Дискреционное управление доступом" снимите галочку в поле "Наследовать...". Откроется диалоговое окно "Разрешения для группы...";

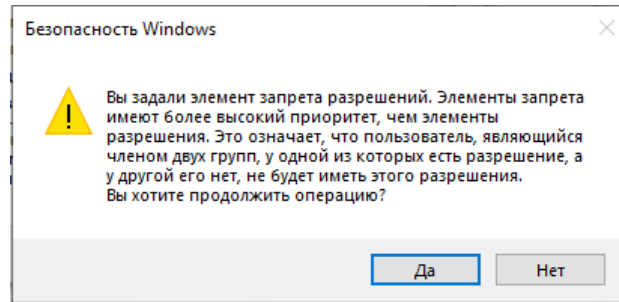


- используя кнопку "Добавить", добавьте пользователей "user1" и "user2" и установите им права доступа в соответствии с таблицей;

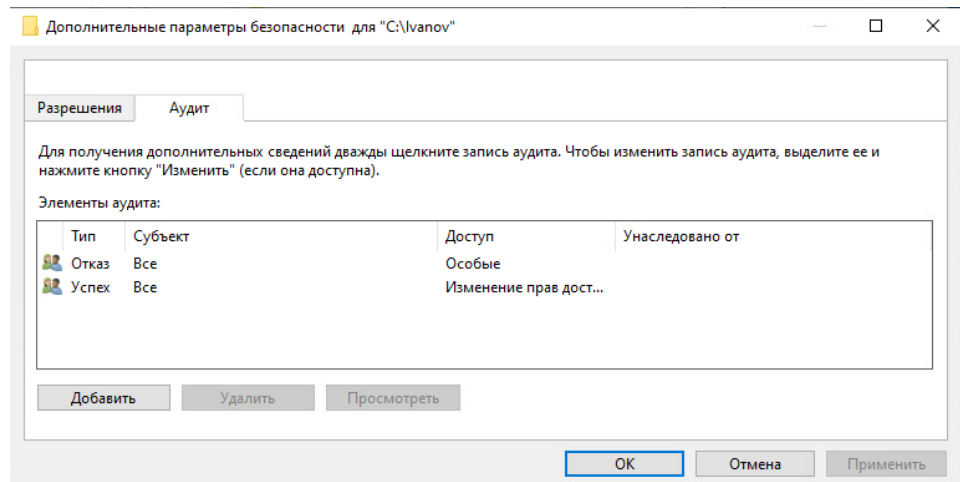


- нажмите кнопку "Применить". Поскольку "user1" и "user2" являются членами группы пользователей компьютера, появится сообщение

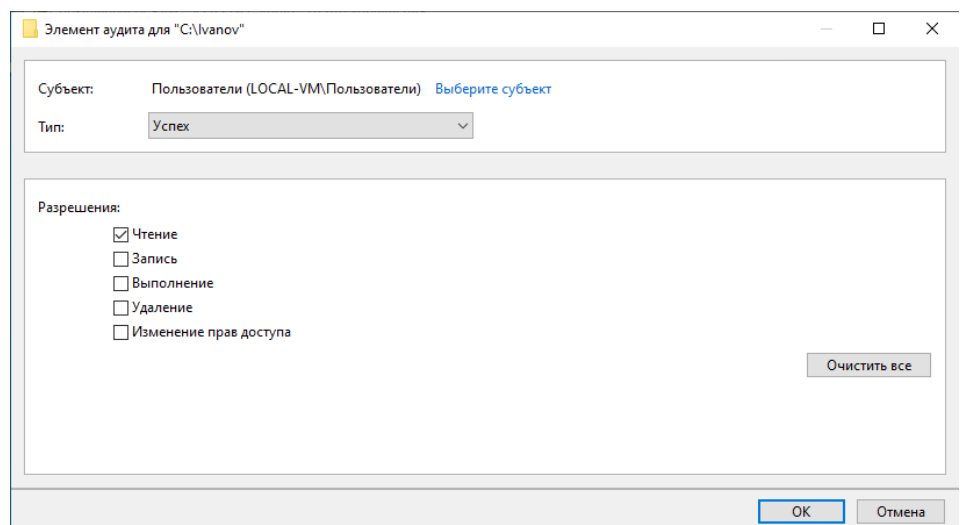
Windows, предупреждающее, что заданная политика запрета приоритетна. Нажмите кнопку "Да". Доступ для папки "C:\Ivanov" задан.



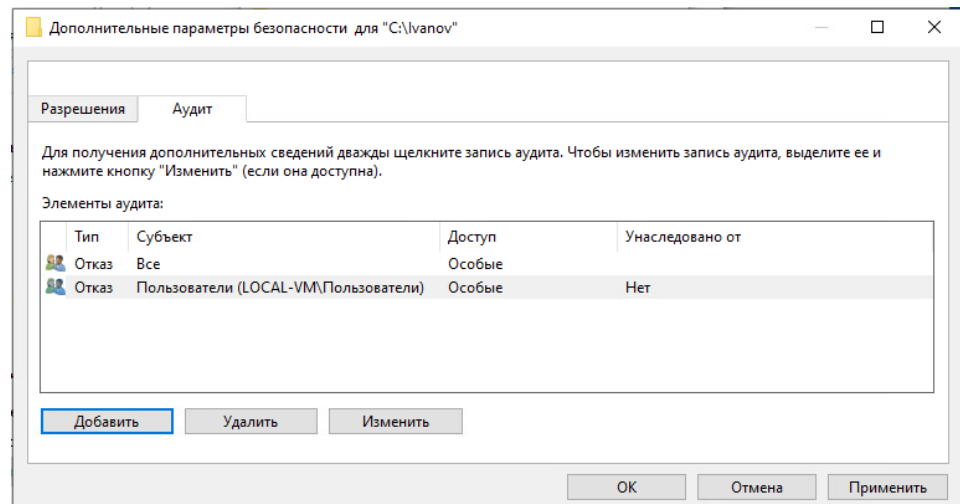
5. Настройте аудит для папки "Ivanov" таким образом, чтобы регистрировались только события отказов в доступе. Для этого в окне "Разрешения для группы ..." нажмите кнопку "Дополнительно". В открывшемся окне "Дополнительные параметры безопасности..." перейдите на вкладку "Аудит" и сделайте следующее:



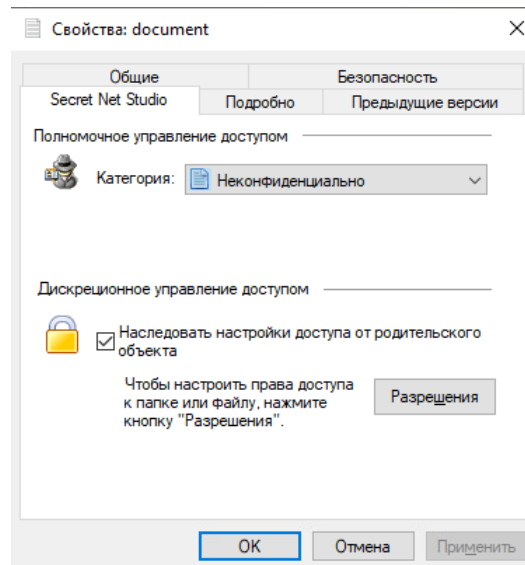
- удалите аудит успеха, выбрав в таблице "Элементы аудита" запись "Успех" и нажав кнопку "Удалить";
- добавьте аудит отказа для группы "Пользователи". Для этого нажмите кнопку "Добавить", выберите группу "Пользователи" и нажмите кнопку "OK". Откроется следующее диалоговое окно "Элементы аудита для...";



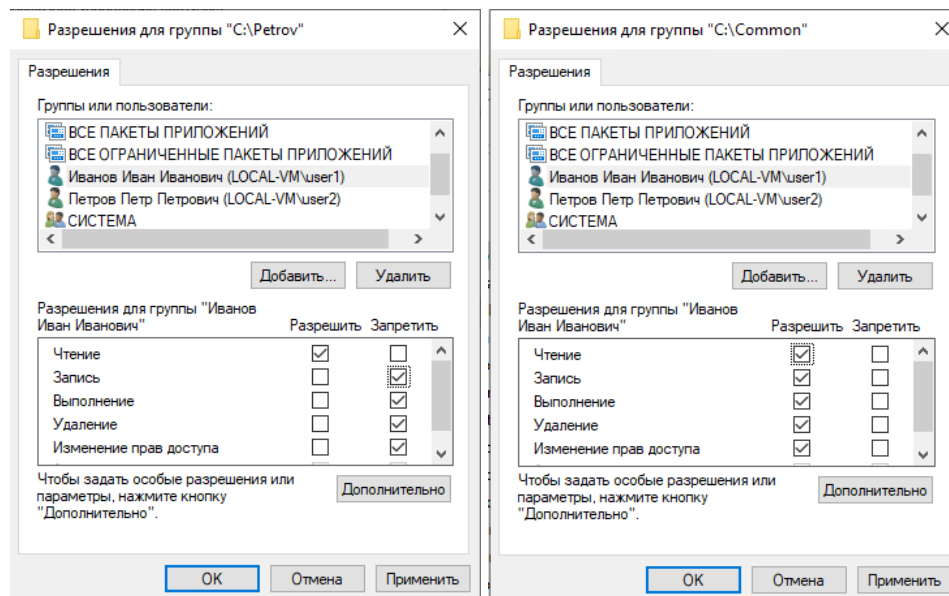
- в поле "Тип" выберите "Отказ", в группе "Разрешения" установите флажки для всех действий и нажмите кнопку "OK". Вы вернулись в окно "Дополнительные параметры безопасности...";



- аудит для папки "Ivanov" настроен. Нажмите кнопку "OK".
6. В окне "Разрешения для группы..." нажмите кнопку "OK". В окне свойств папки также нажмите кнопку "OK".
 7. Таким образом, мы установили параметры доступа к папке "C:\Ivanov" и аудит событий в соответствии с таблицей из п. 4. Откройте папку "C:\Ivanov", вызовите окно свойств файла "document.txt", перейдите на вкладку "Secret Net Studio" и убедитесь, что установлен параметр "Наследовать настройки доступа от родительского объекта" (если данный параметр не установлен, то установите его).

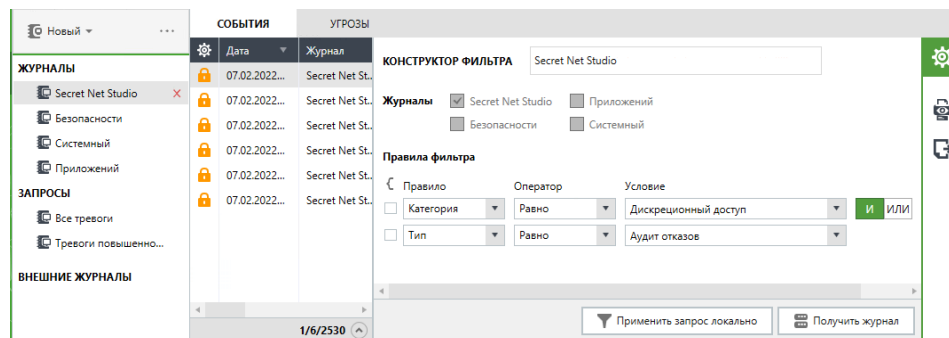


8. Используя описание пп. 4–7, установите в соответствии с матрицей разграничения доступа права доступа и настройку аудита событий для папок "Retrov" и "Common".



9. На компьютере Local-VM завершите работу локальной программы управления и переавторизуйтесь под учетной записью "user1 (Иванов Иван Иванович)". Убедитесь, что пользователю "user1", согласно таблице в п. 4, доступны следующие действия с ресурсами: "C:\Ivanov\document.txt" – чтение и выполнение, "C:\Petrov\graph.txt" – чтение и "C:\Common\plan.txt" – все разрешения.

Переавторизуйтесь с учетной записью "admin", откройте журнал Secret Net Studio и просмотрите события категории "Дискреционный доступ" с типом "Аудит отказов" об отказе в выполнении не разрешенных в соответствии с матрицей доступа (см. п. 4) операций с ресурсами.

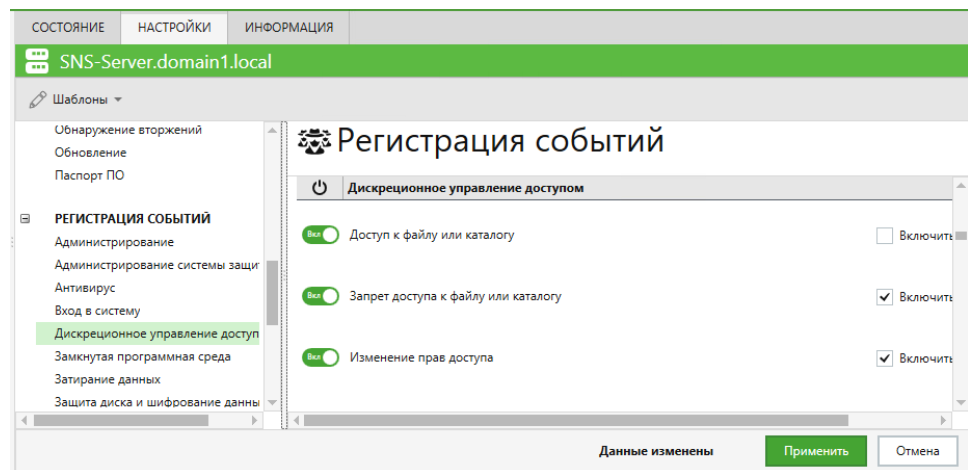
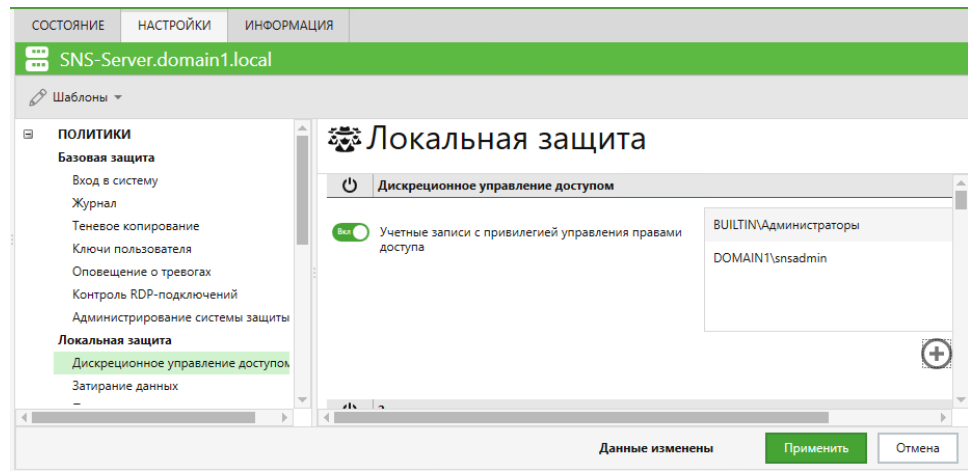


10. Переавторизуйтесь под учетной записью "user2". Убедитесь, что данному пользователю, согласно таблице в п. 4, доступны следующие действия с ресурсами: "C:\Petrov\graph.txt" – чтение, запись и выполнение; "C:\Ivanov\document.txt" – доступ запрещен и "C:\Common\plan.txt" – чтение.

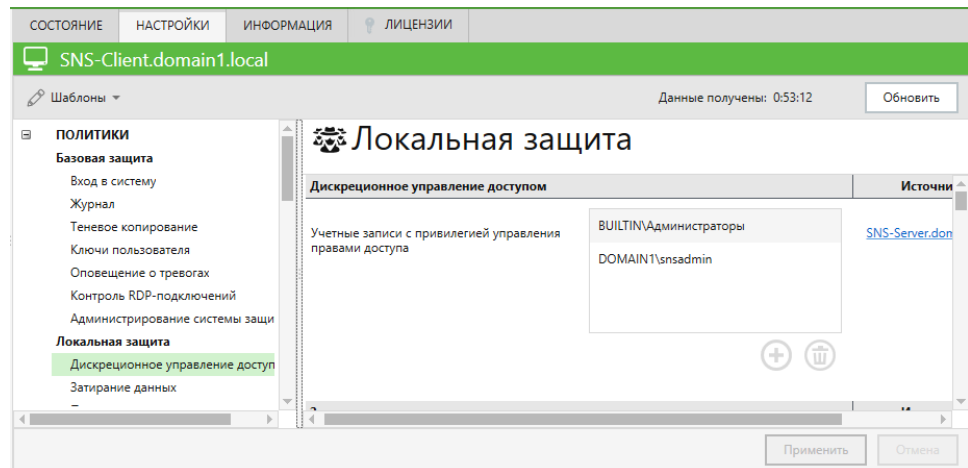
Переавторизуйтесь с учетной записью "admin". Откройте журнал Secret Net Studio и просмотрите события категории "Дискреционный доступ" об отказе в выполнении не разрешенных в соответствии с матрицей доступа (см. п. 4) операций с ресурсами.

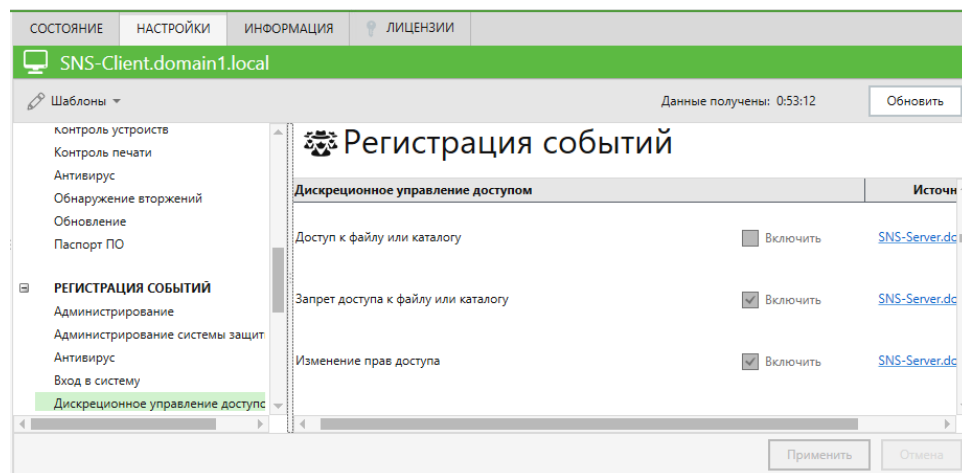
11. Проведите проверку работы дискреционного управления доступом в сетевом варианте. Для этого:

- на VM Admin_VM откройте программу управления в сетевом режиме, выберите объект сервера безопасности и, используя описание п. 3, включите групповую политику дискреционного управления доступом, добавив привилегию на управление правами доступа группе администраторов домена безопасности "snsadmin", а также включите регистрацию событий дискреционного управления доступом;



- примените сделанные изменения. На защищаемых компьютерах SNS-Client и Admin-VM принудительно примените настроенные на сервере безопасности групповые политики с помощью опции контекстного меню "Команды / Применить групповые политики";





- на BM SNS_Server под учетной записью "snsadmin" в общедоступной папке "C:\user_files" создайте защищаемые ресурсы по аналогии с описанием в п. 2:
 - папку "Ivanov" и в ней файл произвольного содержания "document.txt";
 - папку "Petrov" и в ней файл произвольного содержания "graph.txt";
 - папку "Common" и в ней файл произвольного содержания "plan.txt";
- распределите для них права дискреционного доступа для пользователей "user1" и "user2" соответственно матрице разграничения доступа (см. таблицу ниже) и настройте аудит событий, используя описание пп. 4–7;

Пользователи	Документы		
	C:\Ivanov\document.txt	C:\Petrov\graph.txt	C:\Common\plan.txt
user1	rwX	r	Все разрешения
user2	-	rwX	r

- на BM SNS_Client последовательно переавторизуйтесь под учетными записями "user2" и "user1", сделайте попытку доступа к созданным на предыдущем шаге защищаемым ресурсам компьютера SNS-Server и сравните результат;
- на BM SNS_Server в программе "Локальный центр управления" откройте журнал Secret Net Studio и просмотрите события категории "Дискреционный доступ" с типом "Аудит отказов".

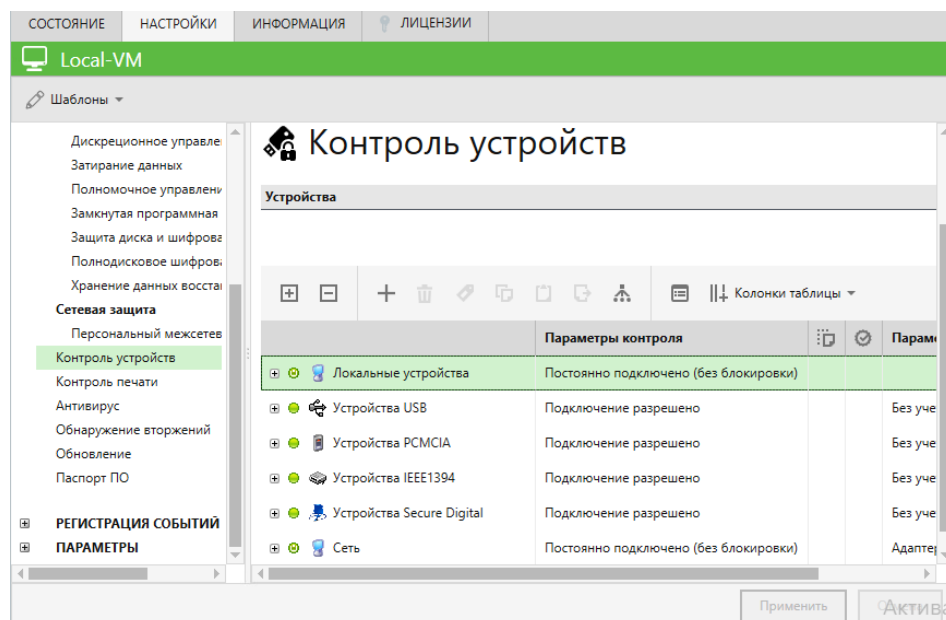
Выполнение сценария завершено.

Сценарий №8 "Управление доступом к съемным носителям информации"

В данном сценарии рассматривается работа механизма управления доступом к подключаемым USB-флеш-накопителям в рамках подсистемы контроля устройств.

Настройку политики контроля устройств можно выполнить либо индивидуально для каждого устройства, либо для модели, класса или группы устройств с использованием принципа наследования параметров.

1. На BM Local_VM убедитесь, что авторизация в ОС выполнена с учетной записью администратора "admin", и подключите USB-флеш-накопитель, который будет использоваться в сценарии для проверки действия механизма контроля устройств.
2. Загрузите список устройств, просмотрите сведения о подключенном USB-флеш-накопителе и настройте политики его контроля. Для этого:
 - в программе "Локальный центр управления" в панели свойств компьютера выберите группу "Политики / Контроль устройств" и прокрутите содержимое окна к таблице "Устройства";



- просмотрите список устройств. Обратите внимание, что в него автоматически добавлены все обнаруженные устройства компьютера. Отключенные в данный момент устройства отображаются с зачеркнутыми именами. Для удобства просмотра списка и оперативного получения основных сведений о текущей конфигурации параметров устройств предусмотрены специальные значки статуса:



– параметры контроля для устройства наследуются от вышестоящего элемента списка устройств;



– режим контроля для устройства отключен;



– включен режим контроля, при котором устройство должно быть постоянно подключено к компьютеру;



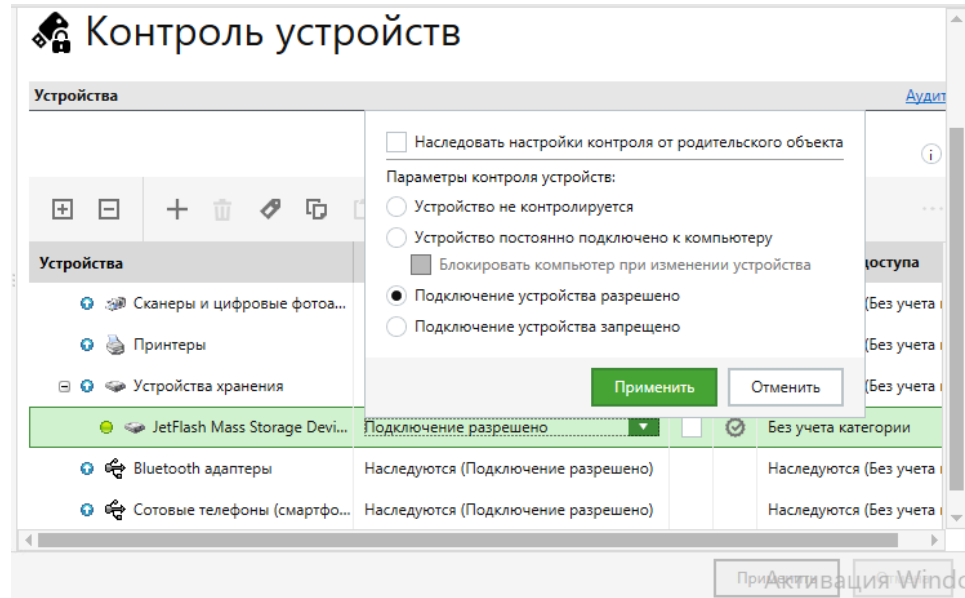
– включен режим контроля, при котором устройство разрешается подключать к компьютеру и отключать;



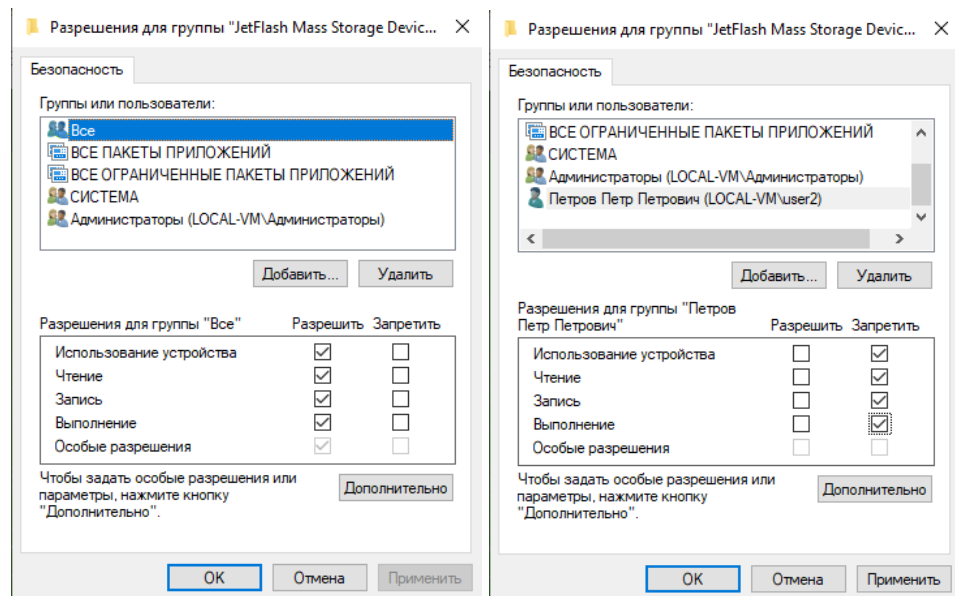
– включен режим контроля, при котором устройство запрещается подключать к компьютеру;

- в таблице "Устройства" выберите "Устройства USB / Устройства хранения / <подключенное устройство>" и раскройте поле "Параметры контроля". Убедитесь, что параметр "Подключение устройства разрешено" установлен, а "Наследовать настройки контроля от родительского объекта" – нет.

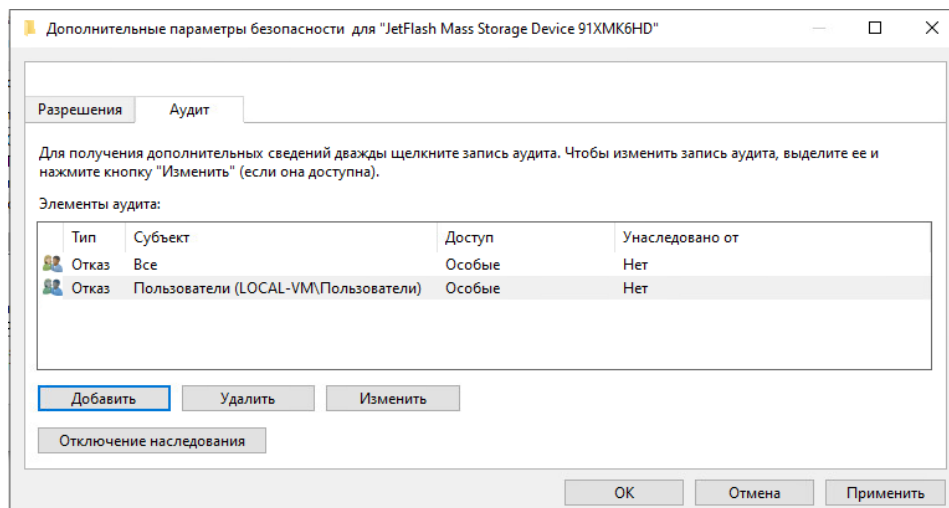
Текущее состояние устройства означает, что включен режим контроля, при котором устройство разрешается подключать к компьютеру и отключать. В случае изменения состояния устройства в журнале регистрируются соответствующие события. Утверждение изменений аппаратной конфигурации при этом не требуется. Данное состояние USB-флеш-накопителя нас устраивает;



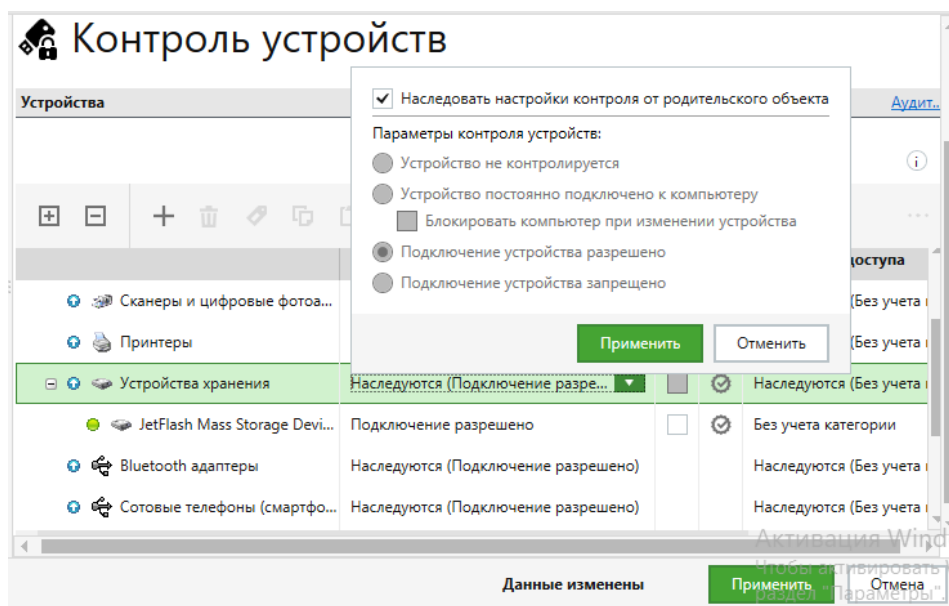
- закройте поле "Параметры контроля" и справа от него нажмите кнопку "Разрешения" . Откроется диалоговое окно "Разрешения...", которое позволяет задавать параметры доступа к этому устройству. Следует иметь в виду, что настройка разрешений и запретов предусмотрена только для портов, дисков и носителей данных (кроме системного диска – для него управление разрешениями запрещено);
- в список "Группы или пользователи" добавьте пользователя "user2 (Петр Петрович Петров)" и установите ему запрет на работу с подключенным в данный момент (именно с этим) USB-флеш-накопителем;



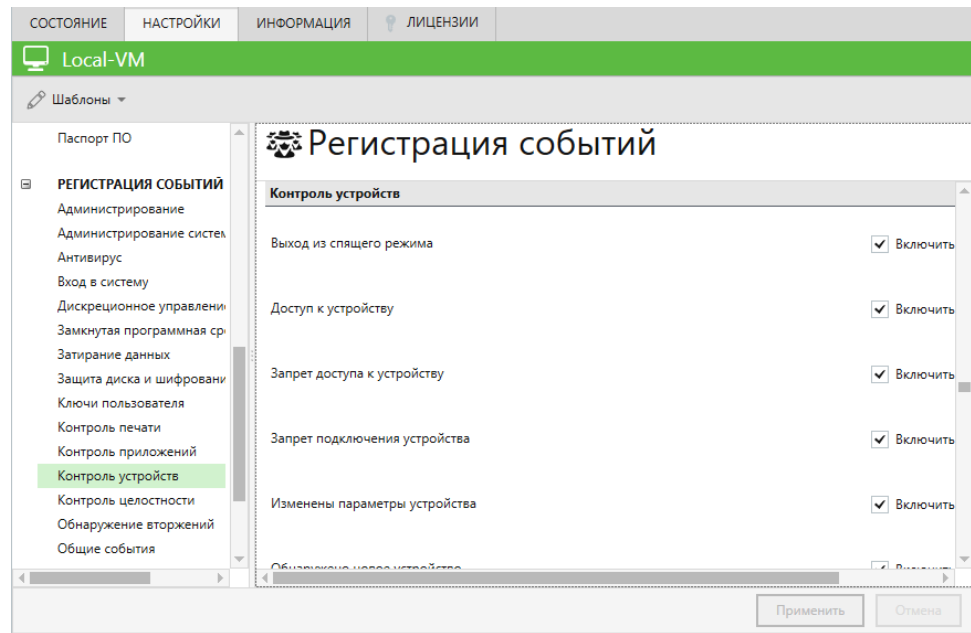
- проведите настройку аудита событий работы с устройством, установив только аудит отказов. Для этого в диалоговом окне "Разрешения..." нажмите кнопку "Дополнительно" и выполните действия, аналогичные описанным в п. 5 предыдущего сценария;



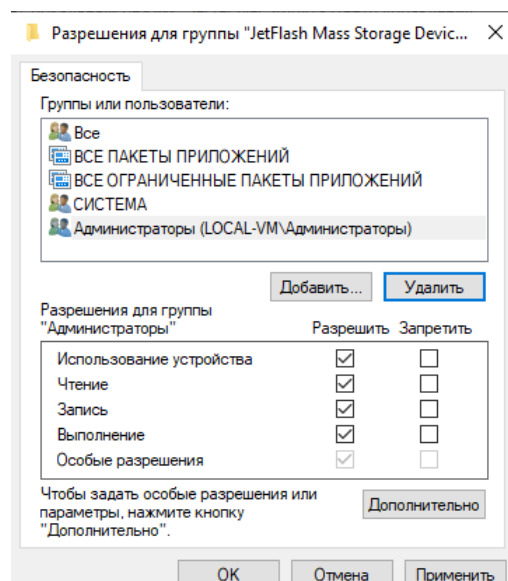
- политики контроля подключенного USB-флеш-накопителя настроены. Последовательно закройте диалоговые окна "Дополнительные параметры безопасности..." и "Разрешения..." и вернитесь в окно программы управления к перечню параметров "Контроль устройств".
3. Установите запрет всем пользователям на использование незарегистрированных USB-флеш-накопителей (всех, кроме подключенного в настоящий момент). Для этого:
- в таблице "Устройства" выберите: "Устройства USB / Устройства хранения" и раскройте поле "Параметры контроля";



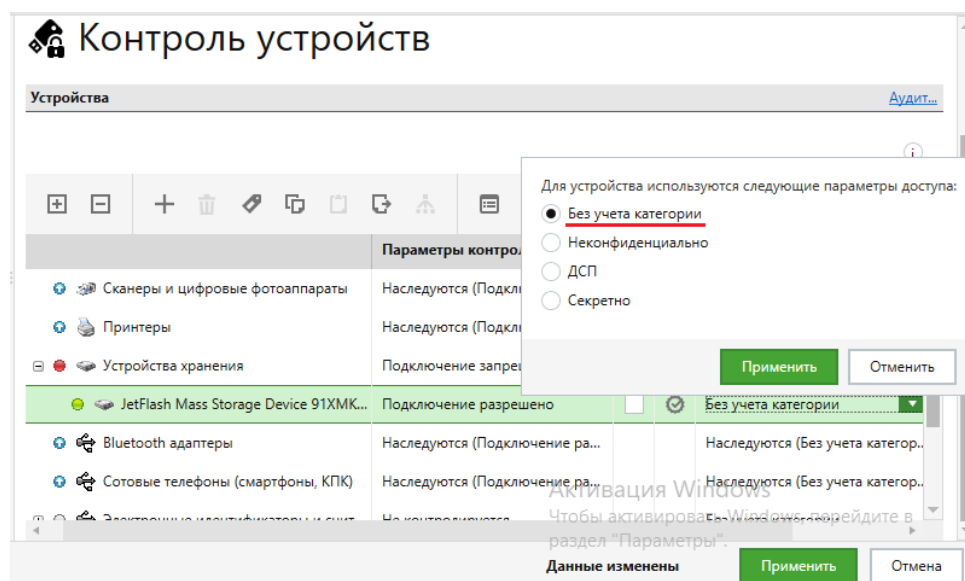
- снимите отметку в поле "Наследовать настройки контроля от родительского объекта" и установите флажок "Подключение устройства запрещено". Нажмите кнопку "Применить";
 - на вкладке "Настройки" нажмите кнопку "Применить". Таким образом, мы запретили всем пользователям использовать незарегистрированные USB-флеш-накопители.
4. Для отслеживания произошедших событий, связанных с работой механизма разграничения доступа к устройствам, следует выполнить настройку регистрации событий. Справа от заголовка группы параметров "Устройства" нажмите кнопку-ссылку "Аудит..." – произойдет переключение в раздел настроек "Регистрация событий / Контроль устройств". Используя кнопку , ознакомьтесь с текущим вариантом настроек и измените их на свое усмотрение.



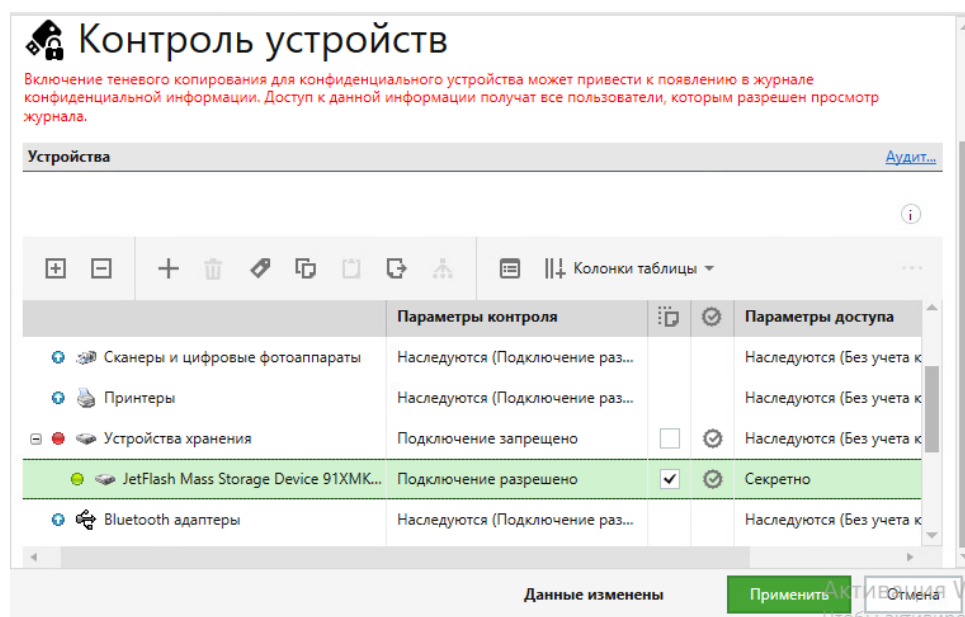
- На VM Local_VM закройте программу управления, переавторизуйтесь под учетной записью пользователя "user2 (Петров Петр Петрович)" и сделайте попытку доступа к подключенному в данный момент зарегистрированному USB-флеш-накопителю. Убедитесь, что в доступе отказано.
- На VM Local_VM переавторизуйтесь под учетной записью пользователя "user1 (Иванов Иван Иванович)" и сделайте попытку доступа к подключенному в данный момент зарегистрированному USB-флеш-накопителю. Убедитесь, что доступ разрешен.
- Протестируйте возможность разграничения доступа к устройству с помощью механизма полномочного управления доступом, присвоив требуемую категорию конфиденциальности. Для этого:
 - на VM Local_VM переавторизуйтесь под учетной записью "admin" и в программе "Локальный центр управления" в панели свойств компьютера выберите в группе параметров "Политики / Контроль устройств" таблицу "Устройства";
 - в таблице "Устройства" выберите "Устройства USB / Устройства хранения / <подключенное устройство>" и справа от него нажмите кнопку "Разрешения". В открывшемся диалоговом окне "Разрешения..." в списке "Группы или пользователи" удалите запрет на работу с подключенным в данный момент флеш-накопителем для пользователя "user2 (Петров Петр Петрович)" и нажмите кнопку "OK";



- в таблице "Устройства" для записи подключенного устройства раскройте поле "Параметры доступа". Текущее значение "Без учета категории" означает, что устройство должно функционировать независимо от уровня допуска пользователя;



- выберите параметр "Секретно" и нажмите кнопку "Применить". В поле "Теневое копирование" установите флажок. Ознакомьтесь с появившимся над таблицей "Устройства" текстом предупреждения;

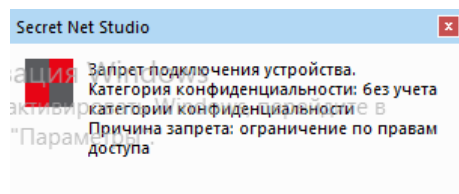


- на вкладке "Настройки" нажмите кнопку "Применить", а затем закройте программу управления;
- сделайте попытку авторизации с учетной записью "user2 (Петров Петр Петрович)" и убедитесь, что в авторизации отказано, поскольку подключено устройство (USB-флеш-накопитель), к которому у пользователя отсутствует доступ (категория конфиденциальности устройства выше, чем у пользователя).

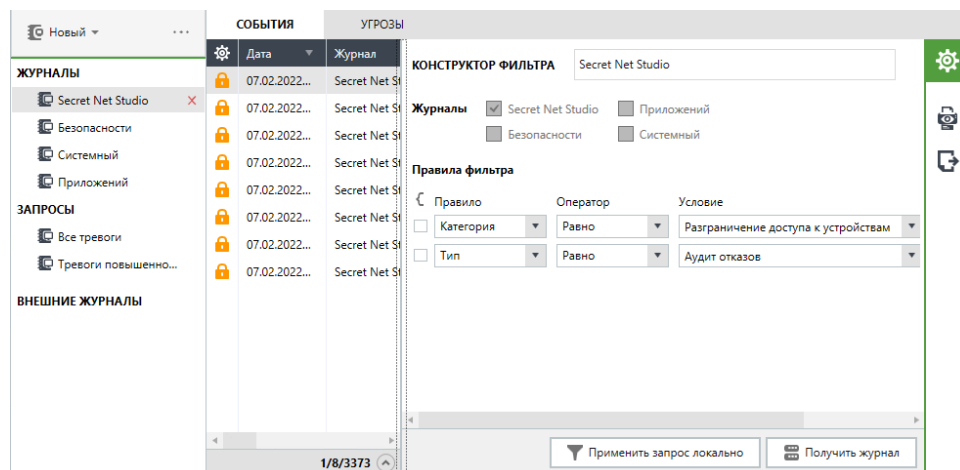
Подробнее о присвоении категорий конфиденциальности устройствам см. в документе "Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация".

8. На VM Local_VM переавторизуйтесь под учетной записью "admin". Отключите зарегистрированный USB-флеш-накопитель и сделайте попытку подключения другого – незарегистрированного – USB-флеш-накопителя. Убедитесь, что подсистема контроля устройств SNS не позволяет подклю-

чить незарегистрированное устройство при работе под любой учетной записью и при этом генерируется событие тревоги.



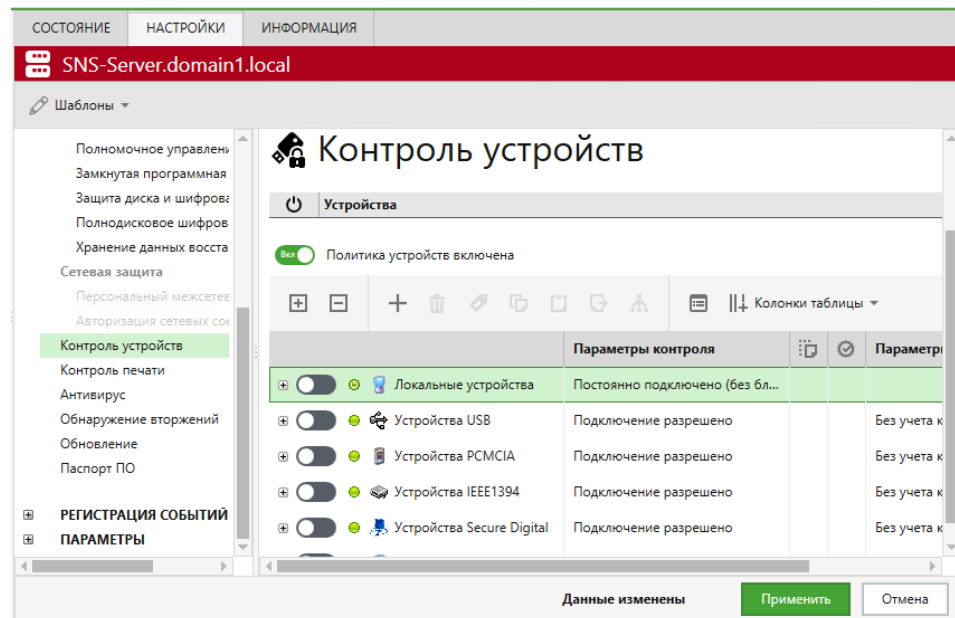
9. На VM Local_VM под учетной записью "admin" откройте журнал Secret Net Studio, просмотрите записи категории "Разграничение доступа к устройствам" с типом "Аудит отказов" и найдите среди них события запрета подключения незарегистрированного USB-флеш-накопителя.



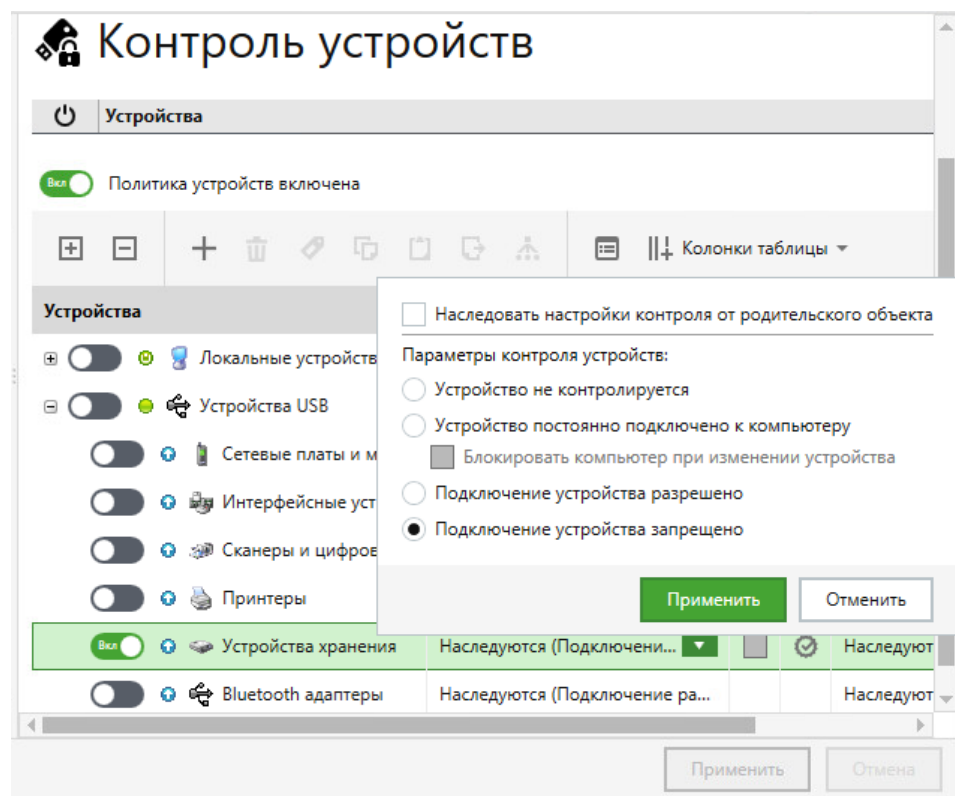
10. На VM Local_VM отмените все заданные ограничения на использование USB-флеш-накопителей.
11. Если на нескольких компьютерах требуется применить одинаковые параметры использования конкретных устройств, можно выполнить их настройку в групповой политике. Устройства, к которым нужно настроить доступ, должны быть добавлены в список групповой политики. При этом в список устройств можно добавить сведения об устройствах, подключенных к клиентскому компьютеру.

Проведите настройку механизма разграничения доступа к устройствам в сетевом варианте – сначала запретите подключение любых USB-флеш-накопителей на защищаемых компьютерах, а затем разрешите подключение одного конкретного устройства:

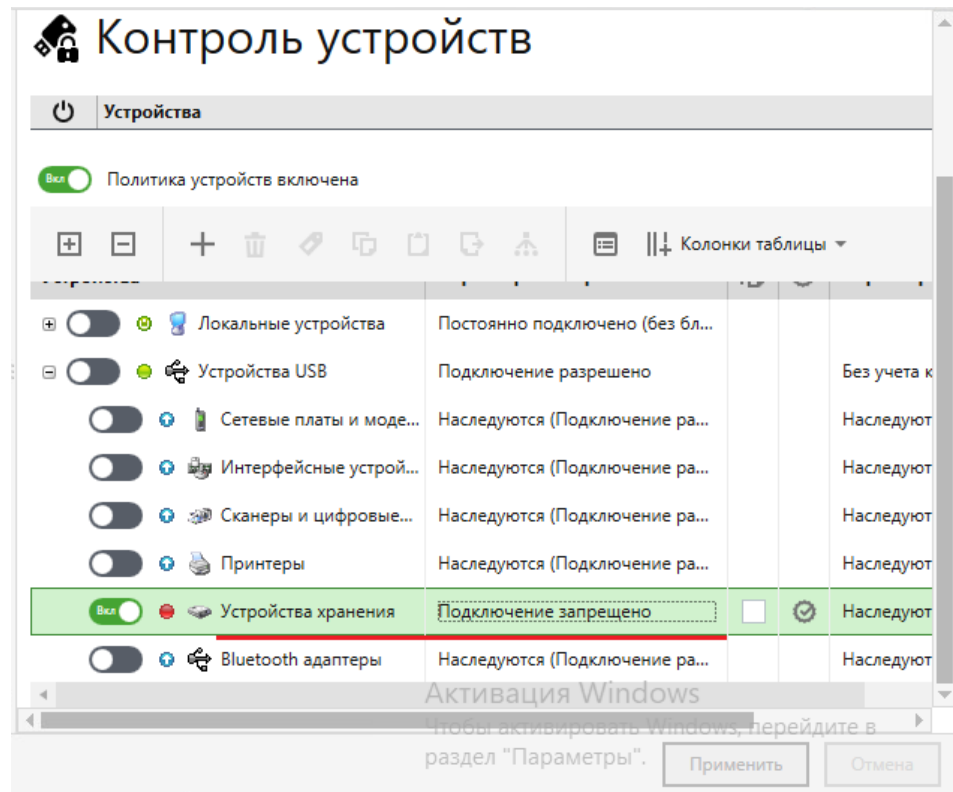
- переключитесь в окно консоли VM Admin_VM. В программе управления в сетевом варианте для объекта сервера безопасности на вкладке "Настройки" включите групповую политику "Контроль устройств";



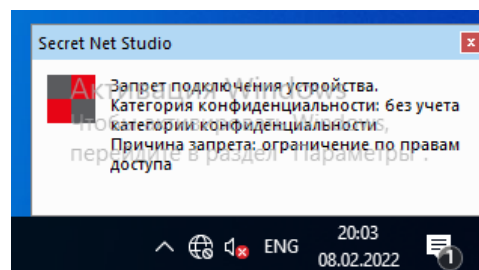
- в таблице "Устройства" включите политику "Устройства USB / Устройства хранения" и примените сделанные изменения;
- в таблице "Устройства" выберите политику "Устройства USB / Устройства хранения", раскройте поле "Параметры контроля", удалите отметку из поля "Наследовать настройки контроля от родительского объекта" и установите флажок "Подключение устройства запрещено";



- примените настройки. Таким образом установлен запрет для всех пользователей на подключение любых USB-флеш-накопителей;



- в программе управления примените групповые политики для объекта SNS-Client, затем откройте консоль VM SNS_Client, переавторизуйтесь под любой доменной учетной записью – "user1 (Иван Иванович Иванов)", "user2 (Петр Петрович Петров)" или "snsadmin" – и убедитесь, что подключение USB-флеш-накопителей запрещено и при этом системой защиты генерируется событие тревоги;



- переключитесь в окно консоли VM Admin_VM. В программе управления откройте "Журналы тревог" (Event Logs), в категории "Стандартные запросы" (Standard queries) выберите запрос "Все повышенного уровня" (All high level) и найдите событие "Запрет подключения устройства" (Device connection prohibition) категории "Разграничение доступа к устройствам" (Device access restriction). Разверните и просмотрите детальные сведения о событии;

Дата	Событие	Категор...	Источник	Комп
08.02.2022...	Запрет подключения устройст...	Разграниче...	LocalProtec...	SNS-Clie...
08.02.2022...	Запрет подключения устройст...	Разграниче...	LocalProtec...	SNS-Clie...
08.02.2022...	Запрет подключения устройст...	Разграниче...	LocalProtec...	SNS-Clie...
08.02.2022...	Базы COB устарели.	Администр...	NetworkPro...	SNS-Clie...
08.02.2022...	Антивирусные базы устарели.	Антивирус	Antivirus	SNS-Clie...
08.02.2022...	Антивирусные базы устарели.	Антивирус	Antivirus	SNS-Serv...

Описание

Запрет подключения устройства.
Категория конфиденциальности: без учета категории конфиденциальности

Причина запрета: ограничение по правам доступа

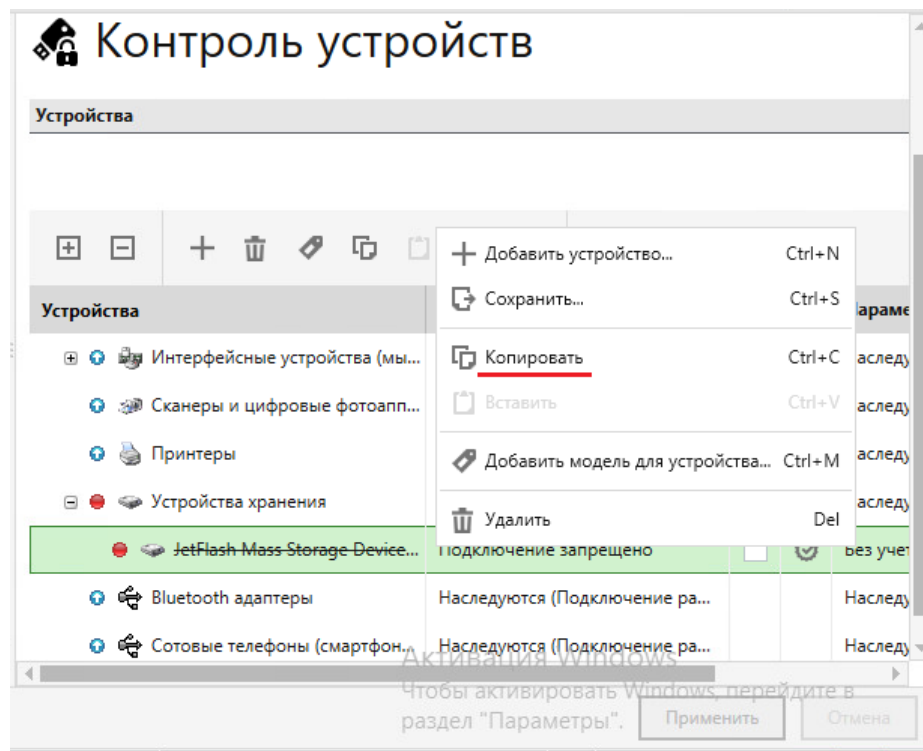
Устройство

JetFlash Mass Storage Device 91XMK6HD

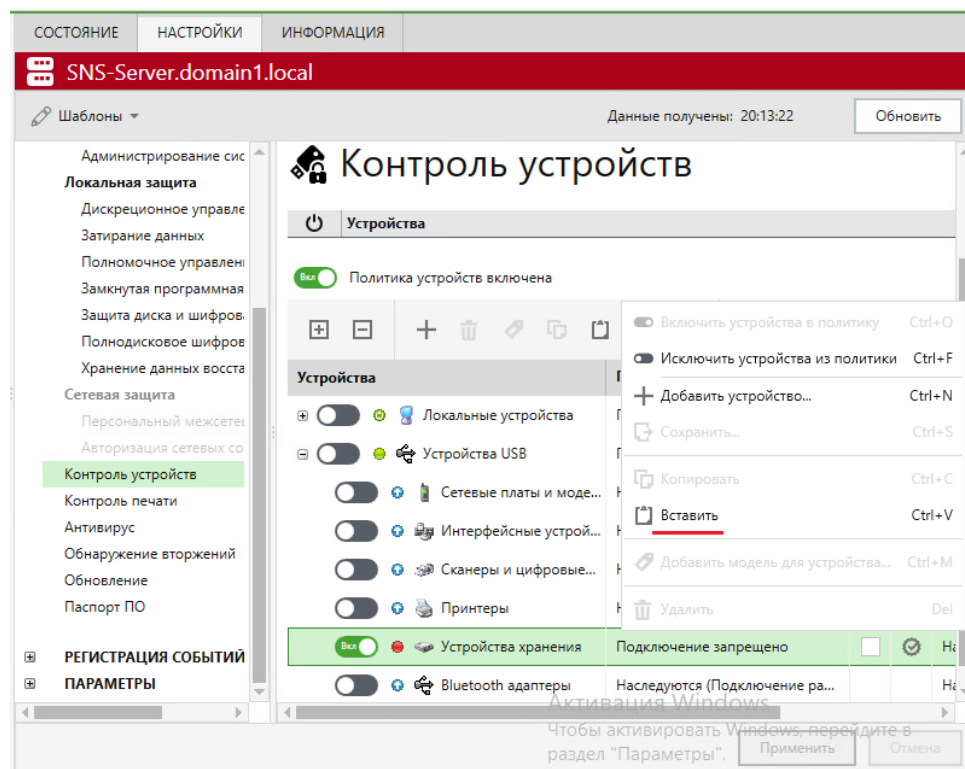
- в программе управления раскройте панель "Компьютеры" , выберите объект SNS-Client и на вкладке "Настройки" выберите группу "Политики / Контроль устройств". В таблице "Устройства" выделите запись "Устройства USB / Устройства хранения / <зачеркнутое наименование устройства>" и убедитесь, что к данному устройству подключение запрещено;

Устройство	Параметры контроля	Параметры
Интерфейсные устройства (мы...	Наследуются (Подключение ра...	Наследу...
Сканеры и цифровые фотоапп...	Наследуются (Подключение ра...	Наследу...
Принтеры	Наследуются (Подключение ра...	Наследу...
Устройства хранения	Подключение запрещено	Наследу...
JetFlash-Mass-Storage-Device...	Подключение запрещено	Без уче...
Bluetooth адаптеры	Наследуются (Подключение ра...	Наследу...
Сотовые телефоны (смартфон...	Наследуются (Подключение ра...	Наследу...

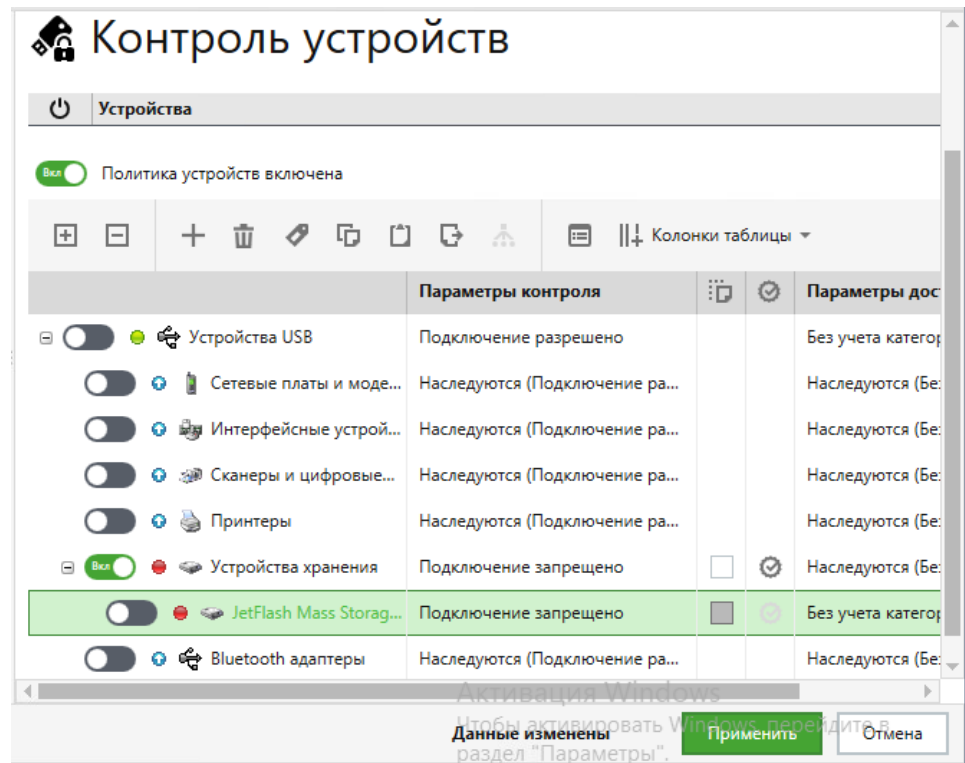
- вызовите контекстное меню этой записи и выберите опцию "Копировать";



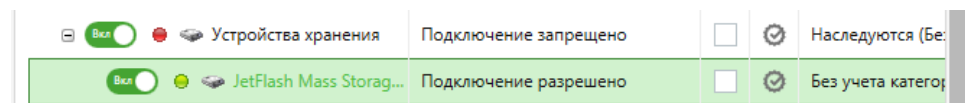
- в программе управления выберите объект сервера безопасности, в настройках политики контроля устройств вызовите в таблице "Устройства" контекстное меню записи "Устройства USB / Устройства хранения" и выберите опцию "Вставить";



- обратите внимание, что в группе "Устройства USB / Устройства хранения" таблицы "Устройства" появилась выделенная зеленым цветом запись с ранее скопированным наименованием из раздела настроек "Контроль устройств" компьютера SNS-Client;



- включите групповую политику добавленного устройства и, используя описание пп. 2 и 3, измените параметры таким образом, чтобы доступ был разрешен всем пользователям, кроме "user2", а затем примените сделанные настройки;



- в программе управления выберите объект компьютера SNS-Client и с помощью опции "Команды / Применить групповые политики" его контекстного меню примените для него групповые политики сервера безопасности.
12. На BM SNS_Client последовательно переавторизуйтесь под учетными записями "user1" и "user2" и протестируйте возможность подключения USB-флеш-накопителя.
 13. Переключитесь в окно BM Admin_VM и в программе управления отмените все сделанные ограничения на использование USB-флеш-накопителей.

Таким образом, рассмотрены примеры настройки механизма управления доступом к подключаемым USB-флеш-накопителям в локальном и сетевом вариантах. Выполнение сценария завершено.

Сценарий №9 "Настройка механизма замкнутой программной среды"

В данном сценарии рассматривается создание замкнутой программной среды для пользователей в автономном и сетевом вариантах использования Secret Net Studio на примере организации возможности запуска только ограниченного набора программ:

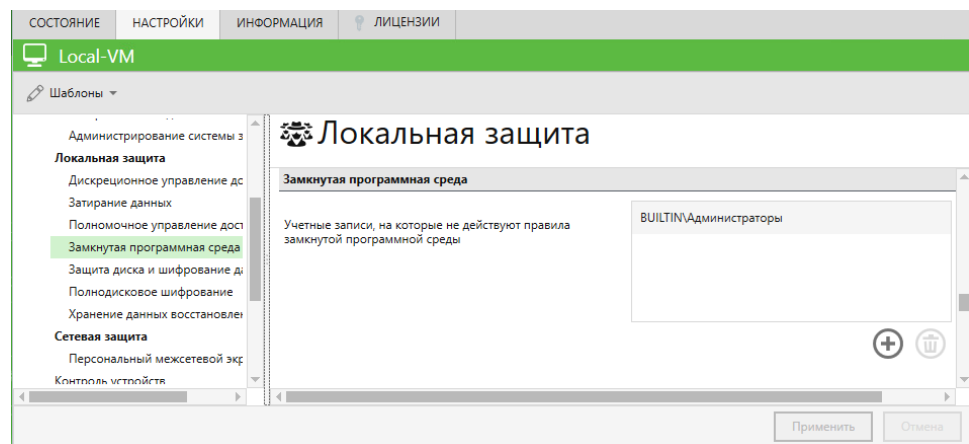
- Проводник;
- MS Wordpad;
- MS Word;
- MS Excel;
- Internet Explorer;
- Корзина.

Модель ЗПС будет создаваться на основе данных журнала Secret Net Studio. В этом случае, чтобы собрать нужные сведения, пользователям разрешается запускать любые приложения. На это отводится некоторый период времени, и запуск приложений регистрируется в журнале. На время сбора сведений необходимо включить регистрацию всех событий категории "Замкнутая программная среда" на тех компьютерах, на которых ЗПС будет использоваться.

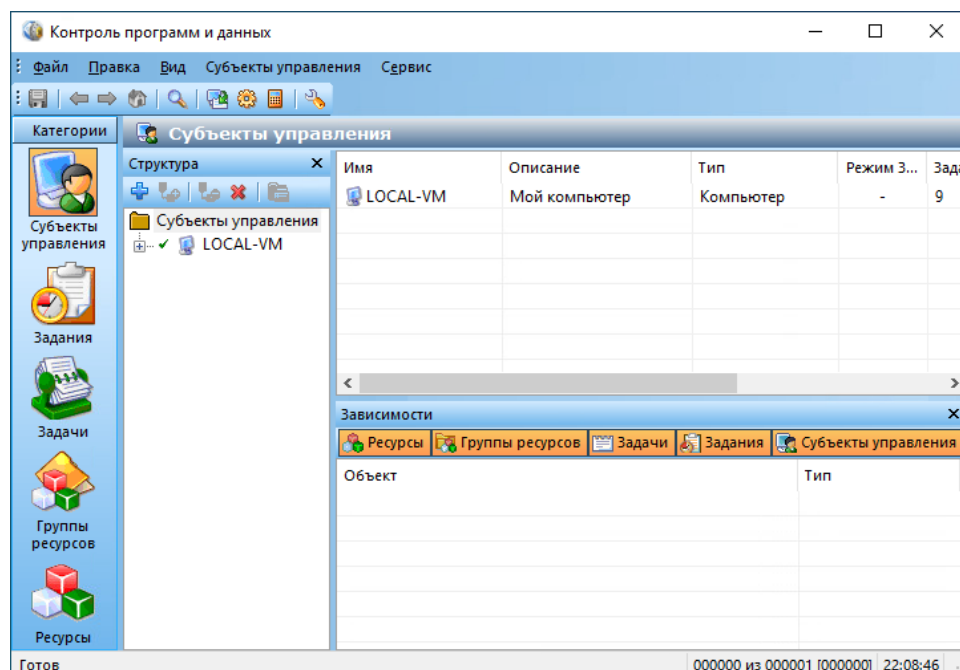
По окончании сбора сведений осуществляется формирование задач ЗПС в модели данных на основе сведений о запускаемых программах из журнала Secret Net Studio. Экспорт сведений в модель данных может выполняться непосредственно из локального журнала Secret Net Studio или из файла, в который предварительно были сохранены записи журнала.

Примечание. Источником при добавлении задач ЗПС по журналу в централизованном режиме является evtx- или snlog-файл, в который предварительно были экспортированы сведения из журнала.

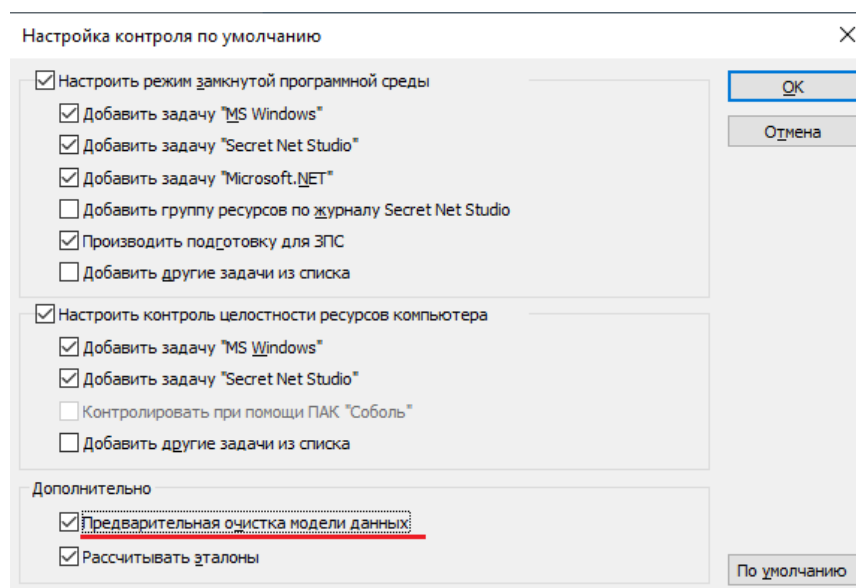
1. В окне консоли VM Local_VM убедитесь, что вы авторизованы под учетной записью "admin". В окне программы управления выберите панель "Компьютер"  и на вкладке "Настройки" раскройте группу "Политики / Локальная защита / Замкнутая программная среда".



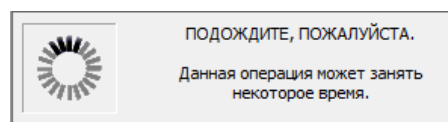
2. Обратите внимание, что в Secret Net Studio используется одна привилегия, связанная с работой ЗПС, – она определяет пользователей, для которых не действуют правила замкнутой программной среды. По умолчанию эта привилегия предоставлена локальной группе "Администраторы". Учетная запись "admin", под которой проводилась установка системы защиты SNS, включена в эту группу.
3. Для настройки механизма ЗПС запустите программу "Контроль программ и данных": "Пуск / Код Безопасности / Контроль программ и данных".

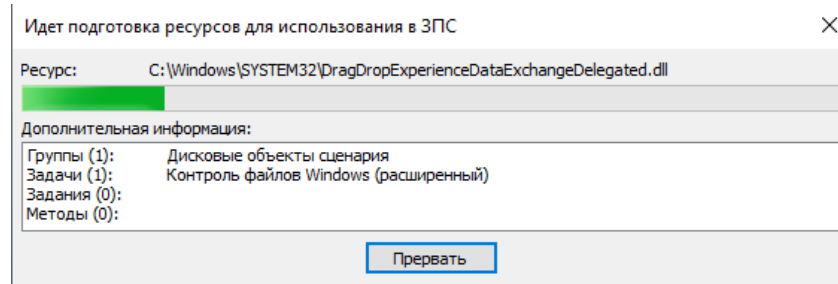


4. Для формирования новой модели данных в главном меню выберите опцию "Файл / Новая модель данных". В открывшемся диалоговом окне "Настройка контроля по умолчанию" установите отметку в поле "Предварительная очистка модели данных".

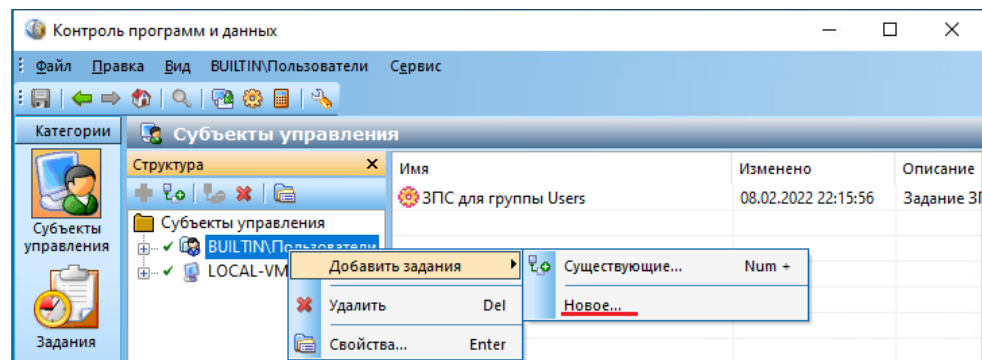


5. Нажмите кнопку "OK". В диалоговом окне подтверждения нажмите кнопку "Да". Предыдущая модель данных будет удалена, и запустится процедура подготовки ресурсов для использования в ЗПС, по окончании которой автоматически запустится расчет эталонов для ресурсов. Дождитесь его завершения.

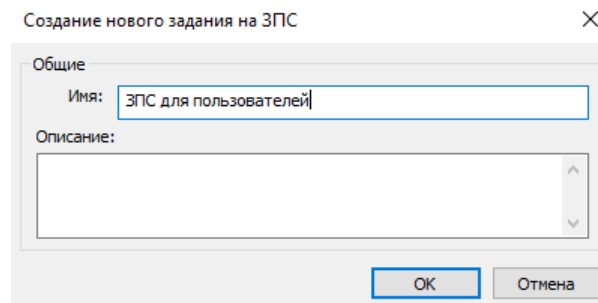




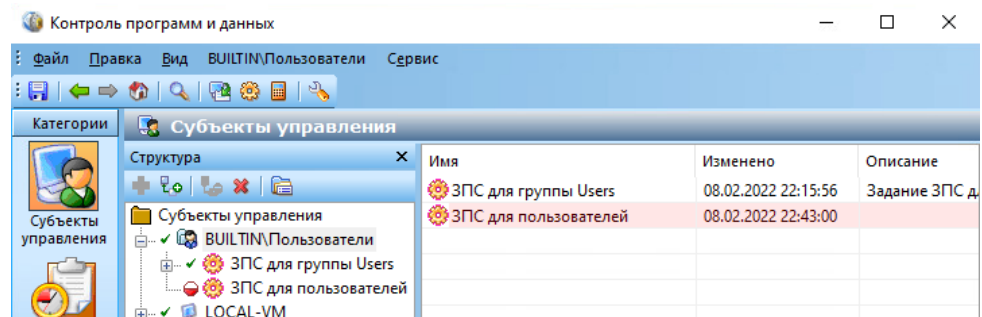
6. После успешного формирования модели данных в основном окне программы управления КЦ-ЗПС появится новая структура объектов. Обратите внимание, что в ней уже содержится сформированное по умолчанию задание, включающее контроль ресурсов самой Secret Net Studio и ОС Windows. Создайте новое задание. Для этого в категории "Субъекты управления" вызовите контекстное меню вновь созданной структуры объектов "BUILTIN\Пользователи" и выберите опцию "Добавить задание / Новое".



7. В открывшемся диалоговом окне введите название **ЗПС для пользователей** и нажмите кнопку "ОК".



8. Обратите внимание, что в окне "Контроль программ и данных" в структуре созданного ранее объекта появилась запись нового задания.



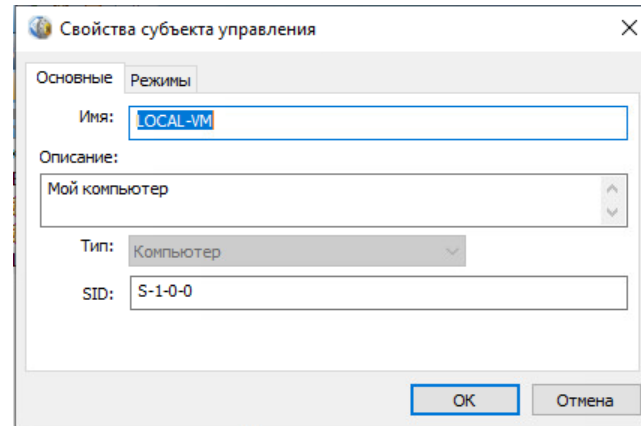
9. Для настройки механизма ЗПС на основе данных журнала Secret Net Studio включите мягкий режим работы ЗПС, в котором пользователю разрешается использовать любые программы. Если при этом запускаются программы, не входящие в перечень разрешенных, – в журнале Secret Net Studio регистрируются события аудита отказа. Это нужно для того, чтобы, не влияя на

работу пользователей, в журнале накопить сведения о возможных ошибках, допущенных при настройке механизма ЗПС, и в последующем их устранить.

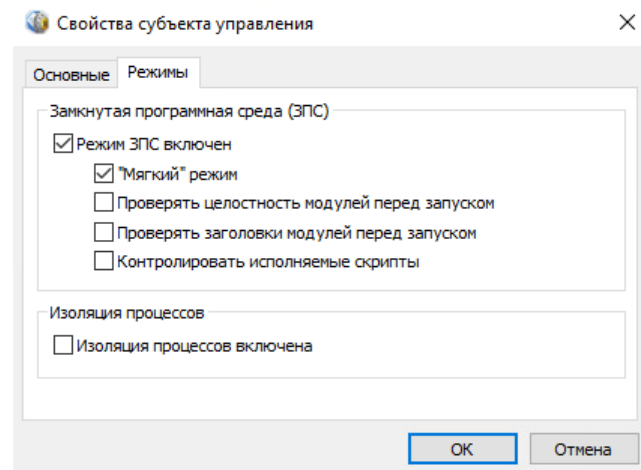
В жестком режиме разрешается запуск только тех программ, которые входят в список разрешенных, а запуск остальных блокируется, и в журнале Secret Net Studio регистрируются события тревоги.

Для включения мягкого режима сделайте следующее:

- в окне "Контроль программ и данных" вызовите контекстное меню субъекта управления "Local-VM" и выберите опцию "Свойства" – откроется диалоговое окно;



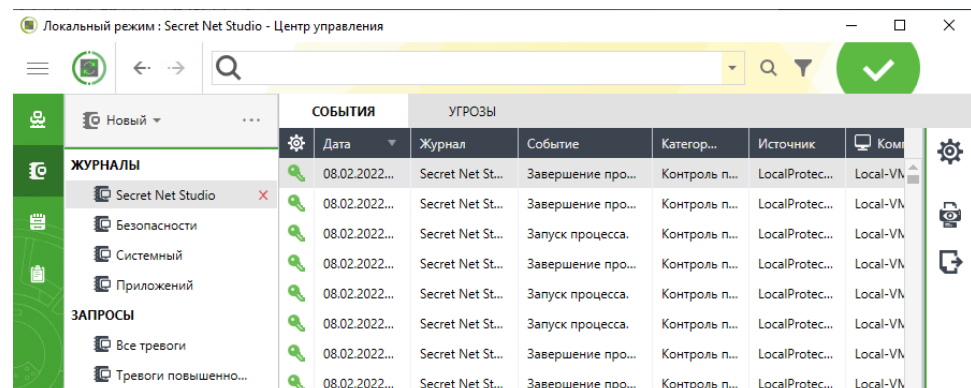
- переключитесь на вкладку "Режимы" и установите отметки в полях: "Режим ЗПС включен" и "Мягкий режим";



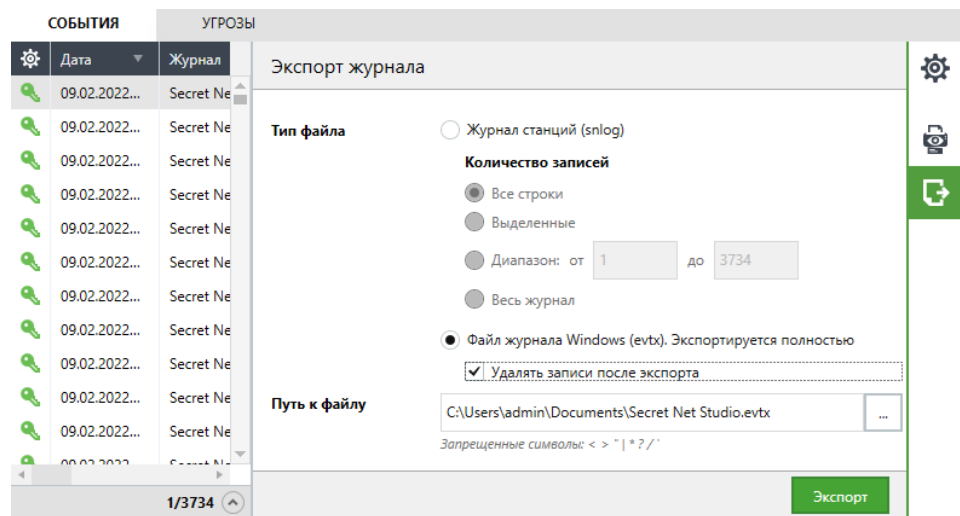
- нажмите кнопку "ОК" и дождитесь завершения сохранения изменений модели данных.

10. Экспортируйте журнал Secret Net Studio во внешний файл, чтобы очистить его. Для этого:

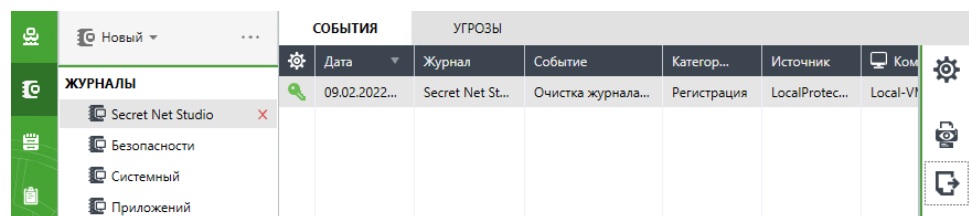
- переключитесь в программу управления и в панели "Журналы" откройте журнал Secret Net Studio;



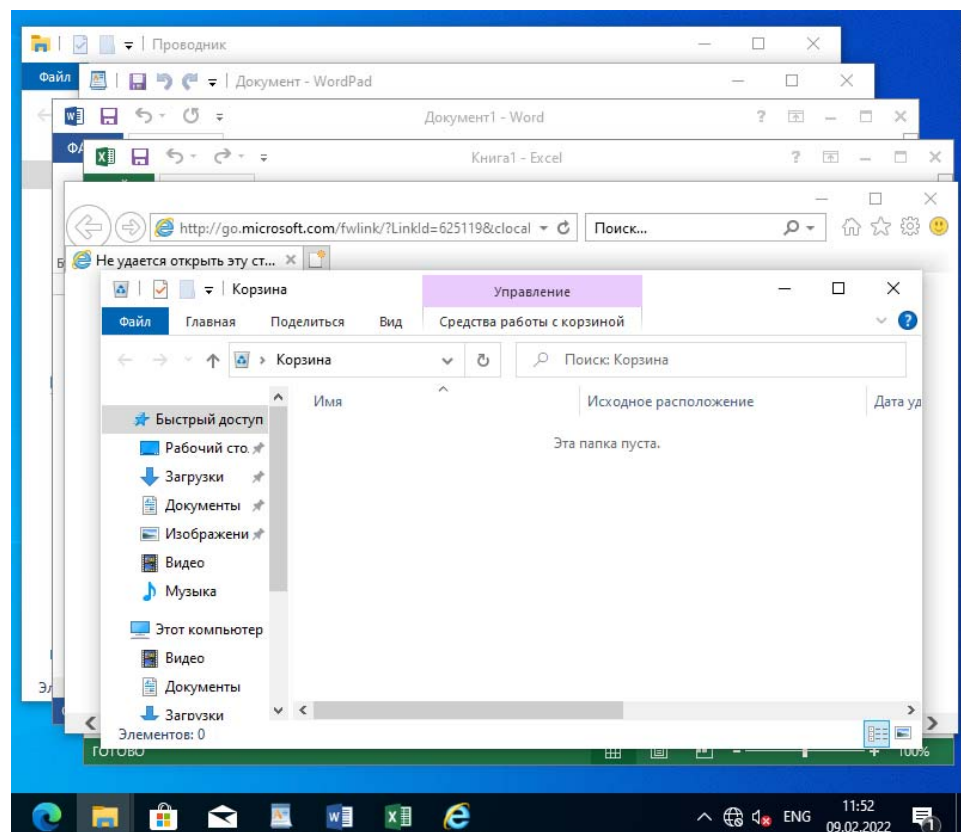
- в правой части окна нажмите кнопку "Экспорт журнала"  и выгрузите журнал Secret Net Studio в файл формата evtx с произвольным наименованием, установив параметр удаления записей при экспорте;



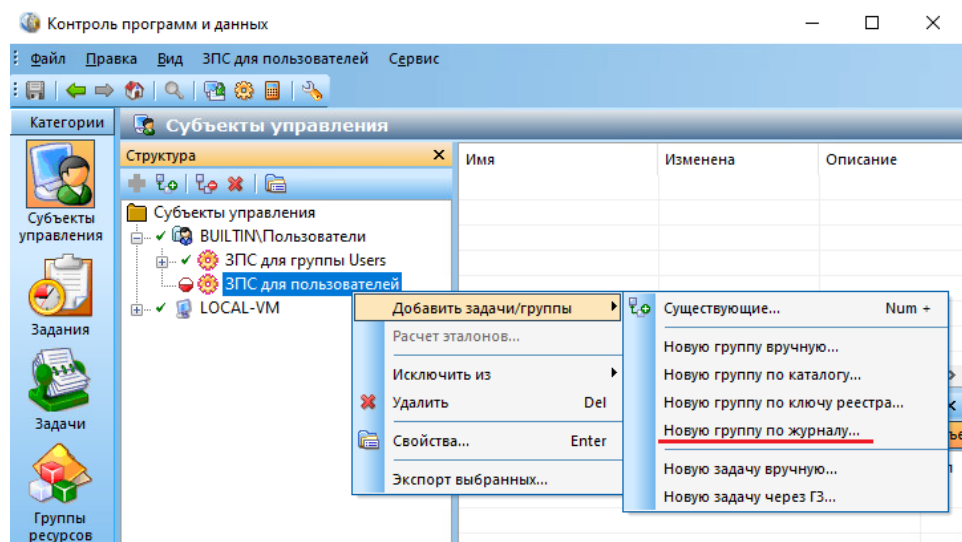
- убедитесь в том, что журнал очищен.



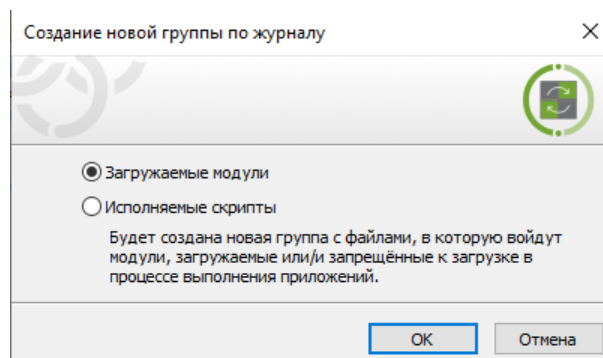
11. Перезагрузите ОС на VM Local_VM и авторизуйтесь под учетной записью "user1 (Иванов Иван Иванович)". Последовательно запустите все программы, которые будут разрешены в дальнейшем пользователям: Проводник, WordPad, MS Word, MS Excel, Internet Explorer, Корзина.



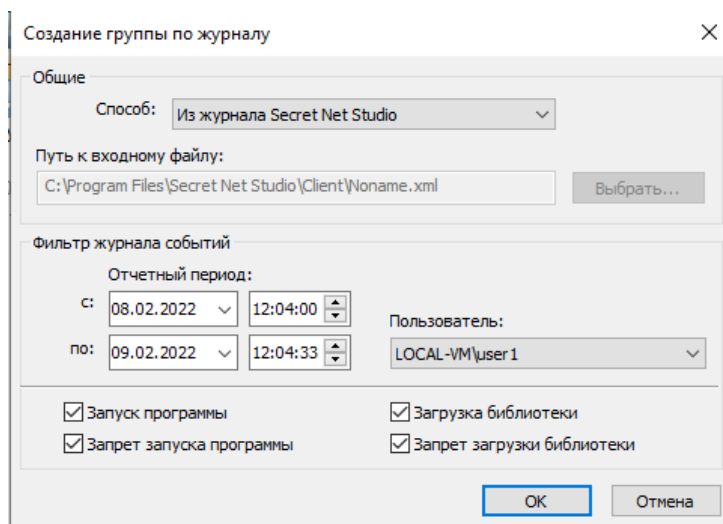
12. Переавторизуйтесь на VM Local_VM под учетной записью "admin" и откройте программу "Контроль программ и данных".
13. К созданному ранее заданию ЗПС добавьте задачи на основании данных из журнала Secret Net Studio. Для этого:
 - выделите запись созданного вами ранее задания "ЗПС для пользователей" и в контекстном меню выберите опцию "Добавить задачи/группы / Новую группу по журналу";



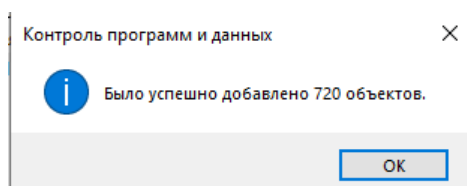
- в открывшемся диалоговом окне убедитесь в том, что выбран переключатель "Загружаемые модули", и нажмите кнопку "ОК".



14. В диалоговом окне "Создание группы по журналу" установите параметры:
 - "Способ" – "Из журнала Secret Net Studio";
 - в поле "Пользователь" нажмите кнопку "Найти" и выберите "user1";
 - в поле "Отчетный период" укажите период запуска разрешенных программ для "user1". Поскольку журнал Secret Net Studio был предварительно очищен, поле "Отчетный период" можно оставить без изменения.

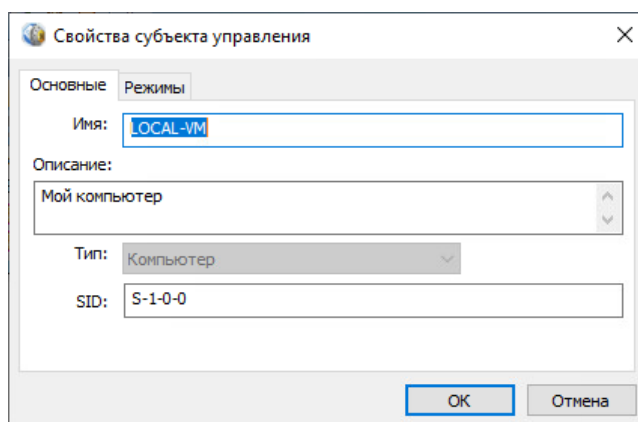


15. Нажмите кнопку "OK" и сохраните сделанные изменения в модели данных.

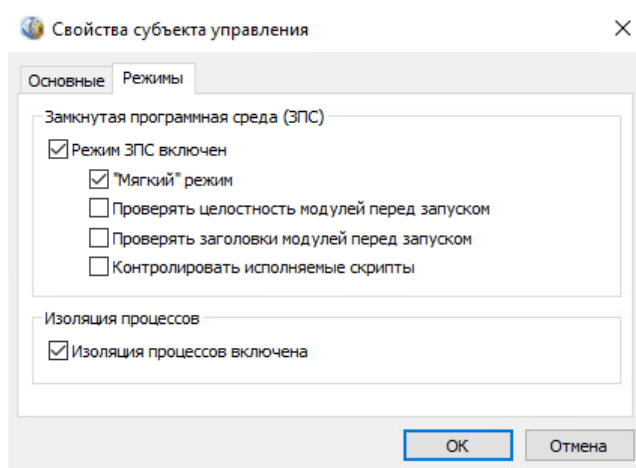


16. Установите запрет обмена данными для приложения WordPad с другими процессами, настроив изоляцию процессов. Для этого:

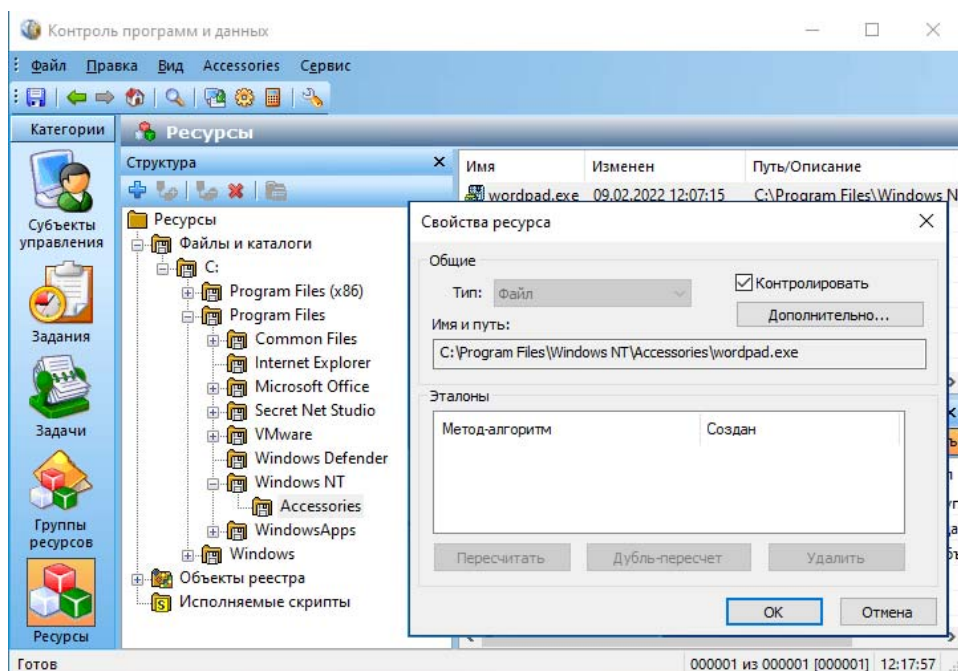
- в окне "Контроль программ и данных" в категории "Субъекты управления" вызовите контекстное меню компьютера Local-VM и выберите опцию "Свойства". Откроется диалоговое окно;



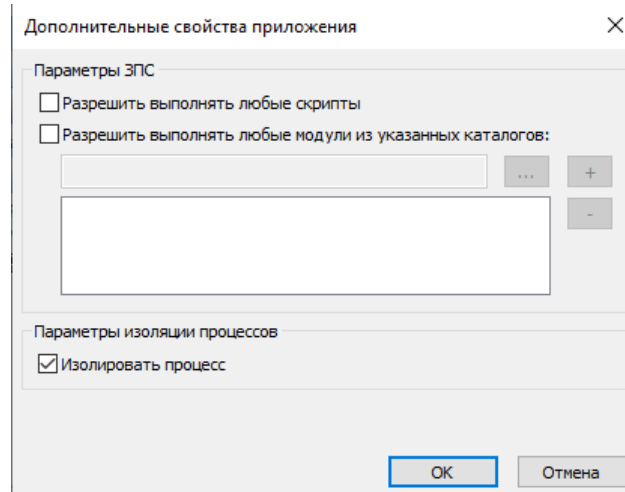
- переключитесь на вкладку "Режимы" и установите отметку в поле "Изоляция процессов включена". Обратите внимание, что механизм изоляции процессов может быть включен независимо от ЗПС;



- нажмите кнопку "OK". Режим изоляции процессов начнет действовать для выбранного компьютера;
- включите изоляцию для ресурса WordPad. Для этого в окне "Контроль программ и данных" выберите категорию "Ресурсы" и раскройте ветку "Файлы и каталоги / C: / Program files / Windows NT / Accessories". Вызовите контекстное меню файла "wordpad.exe" и выберите опцию "Свойства". Откроется диалоговое окно;



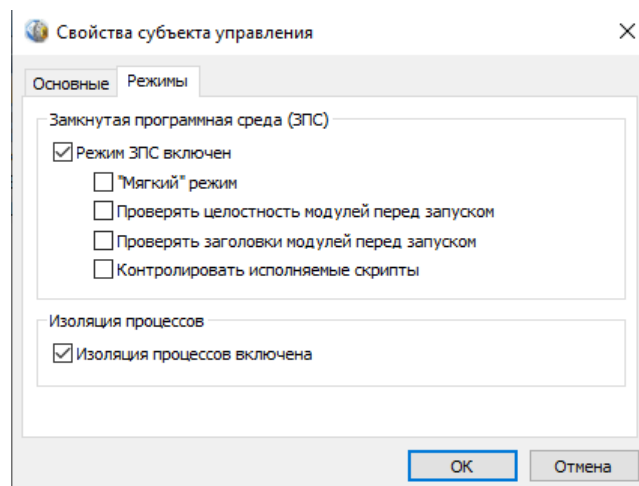
- в диалоговом окне "Свойства ресурса" нажмите кнопку "Дополнительно". В следующем открывшемся окне установите отметку в поле "Изолировать процесс";



- в окнах "Дополнительные свойства приложения" и "Свойства ресурса" нажмите кнопку "ОК". Изоляция для ресурса WordPad включена, и теперь обмен данными между WordPad и другими процессами будет невозможен.

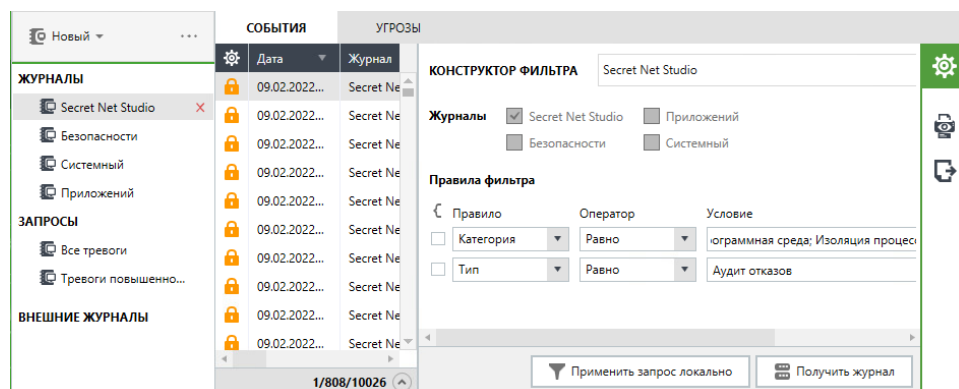
17. Включите жесткий режим для ЗПС. Для этого:

- в окне "Контроль программ и данных" вызовите контекстное меню субъекта управления "Local-VM" и выберите опцию "Свойства";
- в открывшемся диалоговом окне переключитесь на вкладку "Режимы" и снимите отметку в поле "Мягкий режим";



- нажмите кнопку "ОК" и сохраните модель данных.

- 18.** Переавторизуйтесь на VM Local_VM под учетной записью "user1 (Иванов Иван Иванович)" и убедитесь, что пользователь может запускать только ограниченный набор программ: Проводник, WordPad, MS Word, MS Excel, Internet Explorer, Корзина. Попытки запуска других программ, например, Paint, не удаются.
- 19.** Убедитесь, что для приложения WordPad работает механизм изоляции процессов и копирование любых данных из окна WordPad в другие приложения невозможно.
- 20.** Переавторизуйтесь на VM Local_VM под учетной записью "user2 (Петров Петр Петрович)" и убедитесь, что ЗПС работает и для этого пользователя тоже.
- 21.** Переавторизуйтесь на VM Local_VM под учетной записью "admin", в программе управления откройте журнал Secret Net Studio и просмотрите записи категорий "Замкнутая программная среда" и "Изоляция процессов" с типом "Аудит отказов".



22. Откройте программу "Контроль программ и данных", отключите механизмы ЗПС и изоляции процессов, сохраните изменения и перезагрузите VM Local_VM.

23. Самостоятельно. Руководствуясь описанием данного сценария и используя в сетевом варианте ПО "Контроль программ и данных" и "Центр управления", проведите аналогичную настройку механизма ЗПС в централизованном варианте для пользователей "user1 (Иван Иванович Иванов)" и "user2 (Петр Петрович Петров)". Помните, что перед добавлением задач по журналу необходимо из него экспортировать сведения в evtx- или snlog-файл.

Выполнение сценария завершено.

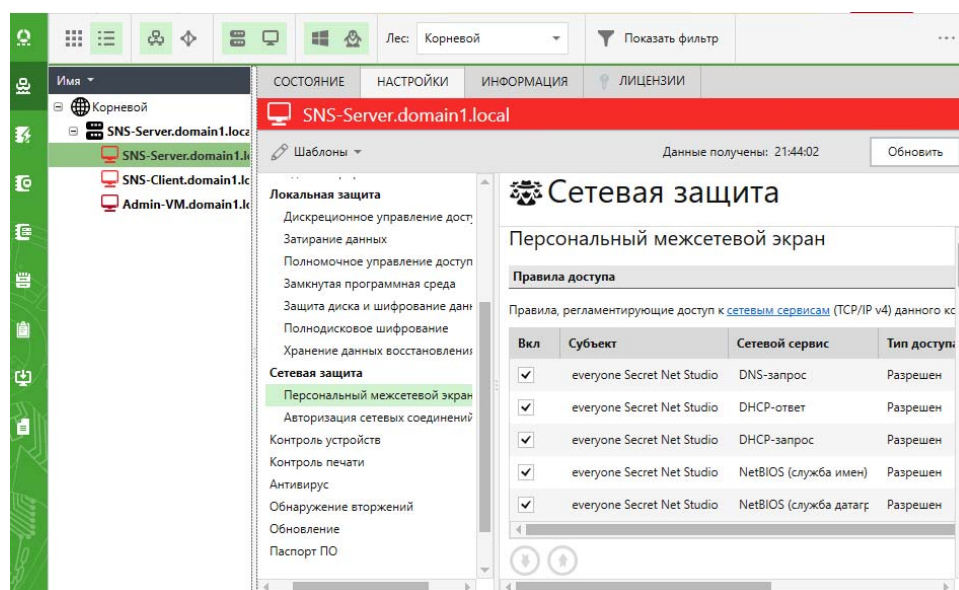
Сценарий №10 "Персональный межсетевой экран"

Настройка межсетевого экрана осуществляется централизованно в программе управления на уровне объектов "Компьютер" по отдельности для каждого из защищаемых компьютеров. Программа управления в локальном режиме непосредственно на защищаемом компьютере позволяет только просматривать централизованно заданные настройки.

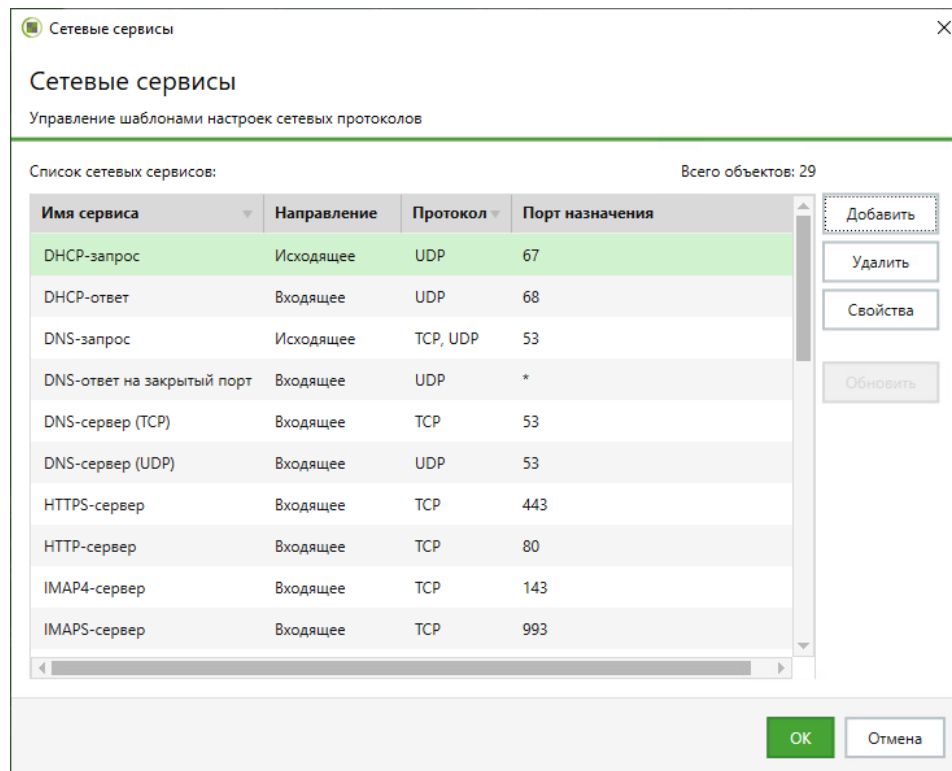
В данном сценарии рассматриваются некоторые практические примеры применения групп правил.

1. Ознакомьтесь с настройками политик МЭ. Для этого в окне VM Admin_VM откройте программу управления в сетевом режиме и выполните следующие действия:

- в панели "Компьютеры" выберите объект агента SNS-Server, раскройте панель его свойств и на вкладке "Настройки" выберите раздел "Политики / Сетевая защита / Персональный межсетевой экран" – в области настроек появятся параметры ПМЭ;



- обратите внимание, что первыми в перечне политик следуют правила доступа, которые регламентируют доступ пользователей к сетевым сервисам защищаемого компьютера. С помощью кнопки  ознакомьтесь с описанием этой группы правил, а затем нажмите над таблицей ссылку сетевых сервисов – откроется диалоговое окно "Сетевые сервисы";



- просмотрите список сетевых сервисов – это шаблоны наиболее распространенных настроек сетевых протоколов. В качестве примера – добавьте новый сетевой сервис для доступа по протоколу/порту TCP/8080. Для этого нажмите кнопку "Добавить" и в открывшемся диалоговом окне заполните следующие параметры:
 - "Тип протокола" – TCP;
 - "Направление" – оставьте вариант "Входящее";
 - "Порт назначения" – введите **8080**. При необходимости можно использовать символ "*" – для всех портов или указать диапазон значений;
 - "Имя сервиса" – **TCP 8080**;
 - параметр "Требовать защищенное соединение" задается, если соединение необходимо устанавливать по защищенному каналу;

- нажмите кнопку "OK". Запись нового сетевого сервиса появится в диалоговом окне "Сетевые сервисы". Далее для созданного сервиса можно написать правила доступа (см. ниже);
- в окне "Сетевые сервисы" нажмите кнопку "OK" и вернитесь к политикам межсетевого экрана.

Для дальнейшего выполнения сценария убедитесь, что RDP-подключение к компьютеру SNS-Server доступно для всех пользователей с BM SNS_Client и Admin_VM. Если это не так, настройте удаленное подключение на сервере SNS-Server.

2. Установите запрет RDP-подключения к серверу SNS-Server с компьютера SNS-Client (192.168.254.110). Для этого добавьте новое правило доступа, выполнив следующие действия:
 - под таблицей "Правила доступа" нажмите кнопку "Добавить" . Откроется окно мастера создания правила. Обратите внимание, что в списке сетевых сервисов отображаются заданные по умолчанию и добавленные администратором вручную сервисы;

Мастер создания правила доступа

Тип доступа

Укажите тип доступа и выберите используемый сетевой сервис.

Доступ: ☒ Разрешить
☐ Запретить

Сетевой сервис Обновить

- NTP-сервер
- POP3S-сервер
- POP3-сервер
- RDP-сервер
- RPC-сервер
- SMB-сервер
- SMTPS-сервер
- SMTP-сервер
- Telnet-сервер
- WINS-репликация
- Все входящие (UDP, TCP)**
- TCP 8080

< Назад Далее > Отмена

- установите параметры: "Доступ" – "Запретить", "Сетевой сервис" – "RDP-сервер". Нажмите кнопку "Далее". На следующем шаге мастера задаются параметры соединения. Их значения по умолчанию соответствуют выбранному на предыдущем шаге сетевому сервису;

Мастер создания правила доступа

Параметры правила

Укажите тип протокола, направление соединения, удаленный порт и приложение, для которого будет действовать правило.

Тип протокола: TCP, UDP

Направление: ☒ Входящее
☐ Исходящее

☒ Требовать защищенное соединение

Порт назначения: 3389 Дополнительно

Приложение: *

< Назад Далее > Отмена

- оставьте заданные по умолчанию параметры правила.

Если необходимо изменить порт, то можно указать нужный номер порта или задать диапазон номеров либо использовать символ "*" (см. п. 1).

В поле "Приложение" можно указать путь к исполняемому файлу, для которого действует правило. При этом можно использовать системные переменные Windows. Символ "*" (звездочка) задает действие для всех приложений. Созданное правило будет анализировать сетевой трафик для приложения, работающего непосредственно на защищаемом компьютере;



Внимание! Для корректной работы правил доступа рекомендуется указывать полный путь к исполняемому файлу приложения.

- нажмите кнопку "Далее". На следующем шаге можно выбрать пользователя или группу пользователей, доступ которой будет контролироваться;

Данная возможность есть только при наличии отдельной лицензии на использование механизма авторизации сетевых соединений. Без такой лицензии в качестве пользователя будет задан "everyone", т.е. фильтрация трафика будет в режиме обычного МЭ.

Мастер создания правила доступа

Субъект доступа

Выберите учетную запись или группу, доступ которой будет контролировать создаваемое правило.

Субъект доступа: everyone Secret Net Studio

Выбрать

< Назад Далее > Отмена

- нажмите кнопку "Далее". На этом шаге мастера можно настроить уведомления о срабатывании правила.

Поле "Выполнить команду" оставьте пустым. Оно используется, если на защищаемом компьютере при срабатывании правила требуется автоматически запускать исполняемый файл. Тогда ниже, в текстовом поле, следует указать полный путь к исполняемому файлу (с параметром), например, C:\windows\notepad.exe 1.txt;

Мастер создания правила доступа

Настройка уведомлений

Укажите способы сигнализации о срабатывании правила.

При наступлении события:

☐ Включить аудит

☐ Звуковая сигнализация

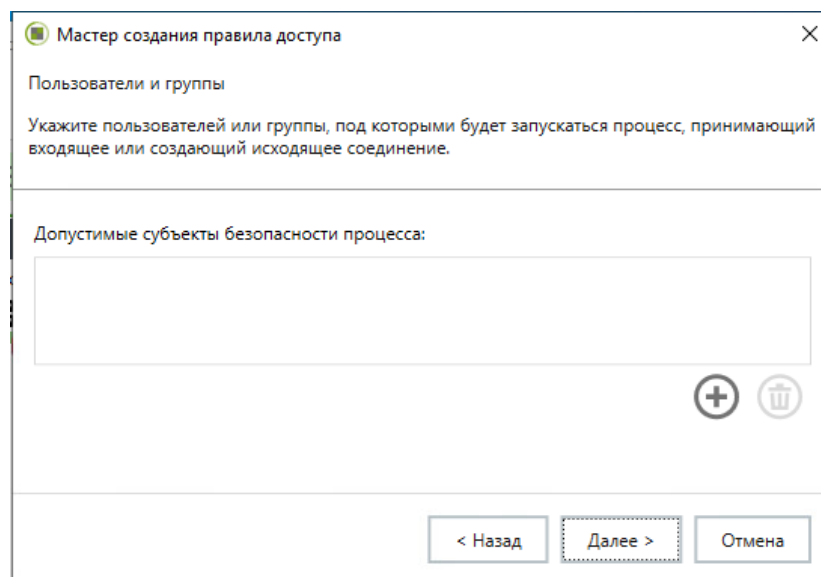
☐ Выполнить команду

в пользовательской сессии: Системной

☐ Запустить с повышенными правами

< Назад Далее > Отмена

- чтобы фиксировать в журнале возникающее при срабатывании правила событие, установите отметку в поле "Включить аудит" и нажмите кнопку "Далее". Появится диалоговое окно для выбора допустимых субъектов безопасности процессов. Здесь через кнопку "Добавить" можно выбрать учетные записи или группы учетных записей, от имени которой будет запущен принимающий входящее соединение или создающий исходящее соединение процесс, для которого будет действовать правило;



- нажмите кнопку "Далее" и на следующем шаге настройте дополнительные параметры правила:
 - "Маска фильтра" – оставьте пустым. При необходимости здесь указывается контекст для поиска IP-пакетов. Правилom будут обрабатываться только IP-пакеты, в теле которых содержится введенное значение;
 - "Удаленный адрес" – введите **192.168.254.110** – IP-адрес компьютера SNS-Client.
Символ "*" задает действие правила для всех адресов. Если нужно указать несколько диапазонов адресов или подсетей, то следует использовать разделитель ";", а сами диапазоны вводить через дефис;
 - "Уведомлять отправителя о блокировке IP-пакета" – оставьте пустым. Поле доступно для изменений в правилах с типом доступа "Запретить" и направлением трафика "Входящее". Если отметка установлена, то отправитель получает уведомления о блокировке пакетов. В случае срабатывания правила для протокола TCP будут генерироваться RST-пакеты, для всех остальных протоколов (кроме ICMP, AH, ESP) – пакеты ICMP (тип Destination Unreachable);

Мастер создания правила доступа

Дополнительные критерии

Укажите дополнительные параметры правила, такие как адреса узлов и маска фильтра.

Маска фильтра:

Удаленный адрес:

Локальный адрес:

☐ Отключить правило

☐ Уведомлять отправителя о блокировке пакета

< Назад Далее > Отмена

- нажмите кнопку "Далее". На завершающем шаге мастера можно настроить расписание работы правила. При этом время работы для правила определяется часовым поясом защищаемого компьютера;

Мастер создания правила доступа

Расписание работы правила

Настройте часы работы создаваемого правила. Для множественного выбора и выбора нескольких областей используйте клавиши CTRL и SHIFT.

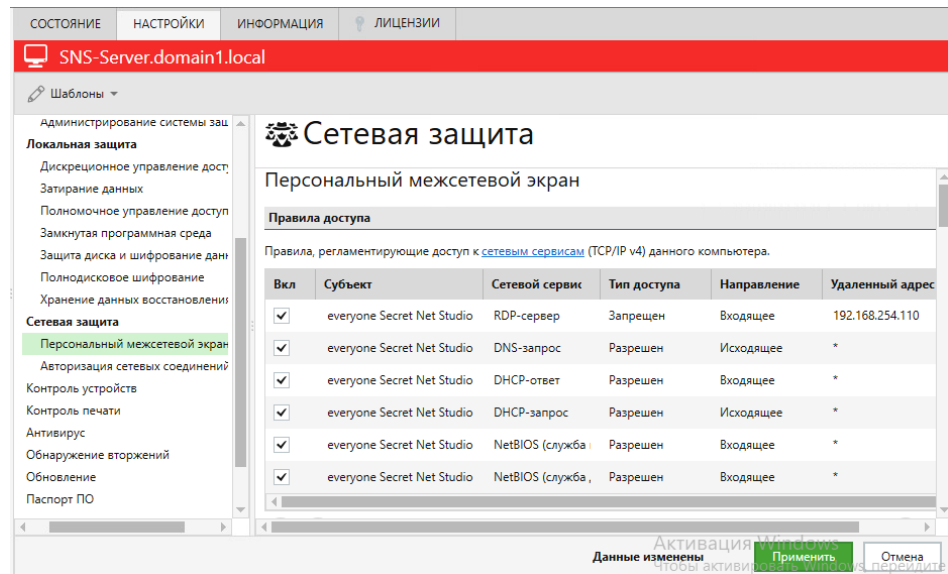
☐ Задать расписание

	Понедельник	Вторник	Среда	Четверг	Пятница	Суббота	Воскресенье
0:00							
1:00							
2:00							
3:00							
4:00							
5:00							
6:00							
7:00							
8:00							
9:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00							

Правило: ☐ активно ☐ не активно

< Назад Далее > Готово Отмена

- нажмите кнопку "Готово". Правило будет создано и отобразится в списке правил. Наивысшим приоритетом обладают правила, расположенные в начальных строках таблицы.



3. Используя описание п. 2, добавьте следующие правила фильтрации доступа для созданного вами ранее сетевого сервиса "TCP 8080":

- запретить доступ к порту TCP/8080 клиентам группы Everyone (для всех пользователей) с произвольными IP-адресами;
- разрешить доступ к порту TCP/8080 клиентам группы Everyone только с компьютера Admin-VM с IP-адресом 192.168.254.101.

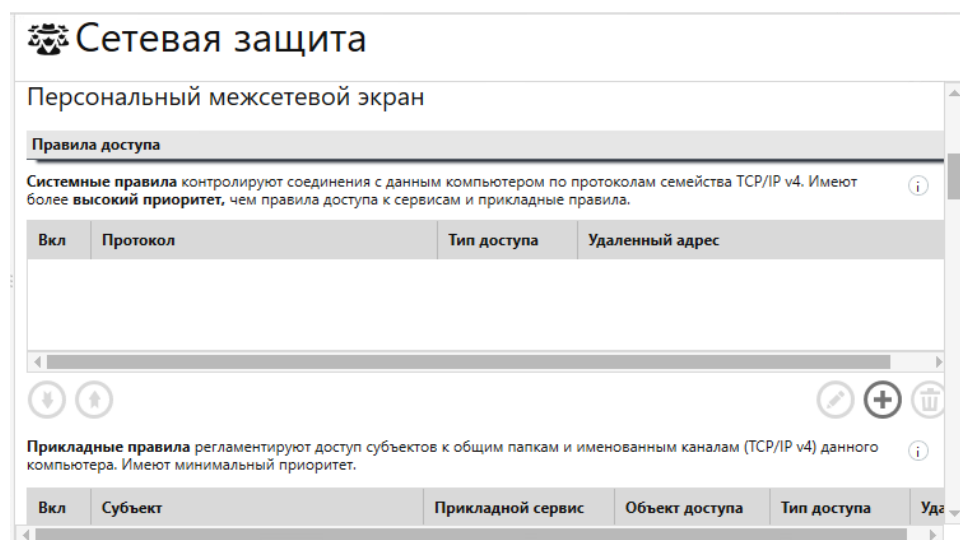
4. С помощью расположенных под таблицей кнопок "Вниз" и "Вверх" установите приоритет разрешающего правила выше, чем запрещающего.

На вкладке "Настройки" нажмите кнопку "Применить". Дождитесь появления в панели событий сообщения о сохранении настроек (возможна некоторая задержка в применении политик межсетевого экранирования на агенте).

Теперь доступ к серверу SNS-Server по порту TCP/8080 будет возможен только с компьютера Admin-VM. В журнале событий Secret Net Studio будут регистрироваться попытки доступа с IP-адресами отправителя и получателя пакетов.

5. Ознакомьтесь с настройками дополнительных категорий правил. Для этого:

- под таблицей "Правила доступа" нажмите кнопку-ссылку "Показать специализированные правила доступа" и прокрутите перечень настроек политик вниз, чтобы увидеть таблицу "Системные правила";



- системные правила являются более общими по сравнению с правилами доступа. Самостоятельно, в качестве примера, добавьте системное правило запрета доступа к серверу SNS-Server по RDP-протоколу, аналогичное описанному в п. 2.

6. Добавьте прикладное правило, запрещающее доступ с компьютера SNS-Client (192.168.254.110) к общедоступной папке "user_files", расположенной на сервере SNS-Server. Для этого под таблицей "Прикладные правила" нажмите кнопку "Добавить"  и в окне мастера создания правила выполните следующие настройки:

- на начальном шаге выберите сервис "Папки общего доступа" и нажмите кнопку "Далее";

Мастер создания прикладного правила

Тип доступа

Укажите тип доступа и имя общей папки.

Доступ: ☒ Разрешить ☐ Запретить

Имя общей папки: *

< Назад Далее > Отмена

- на следующем шаге установите: "Доступ" – "Запретить", "Имя общей папки" – введите **user_files**;
- нажмите кнопку "Далее". На следующем шаге мастера можно выбрать учетные записи, для которых действует правило;

Мастер создания прикладного правила

Субъект доступа

Выберите учетную запись или группу, доступ которой будет контролировать создаваемое правило.

Субъект доступа: everyone Secret Net Studio Выбрать

< Назад Далее > Отмена

- нажмите кнопку "Далее". На следующем шаге нужно настроить уведомления о срабатывании правила. Выберите поле "Включить аудит";

Мастер создания прикладного правила

Настройка уведомлений

Укажите способы сигнализации о срабатывании правила.

При наступлении события:

☒ Включить аудит

☐ Звуковая сигнализация

☐ Выполнить команду

в пользовательской сессии: Системной

☐ Запустить с повышенными правами

< Назад Далее > Отмена

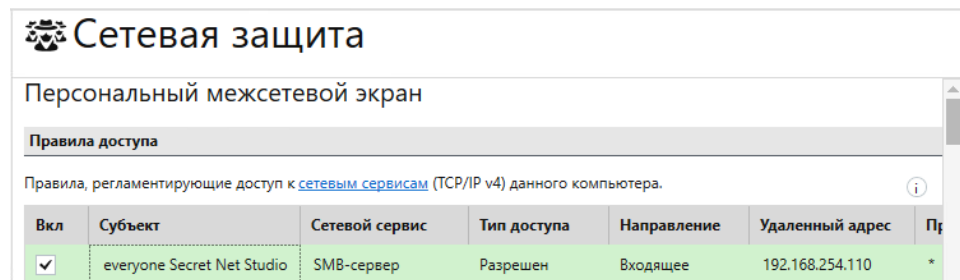
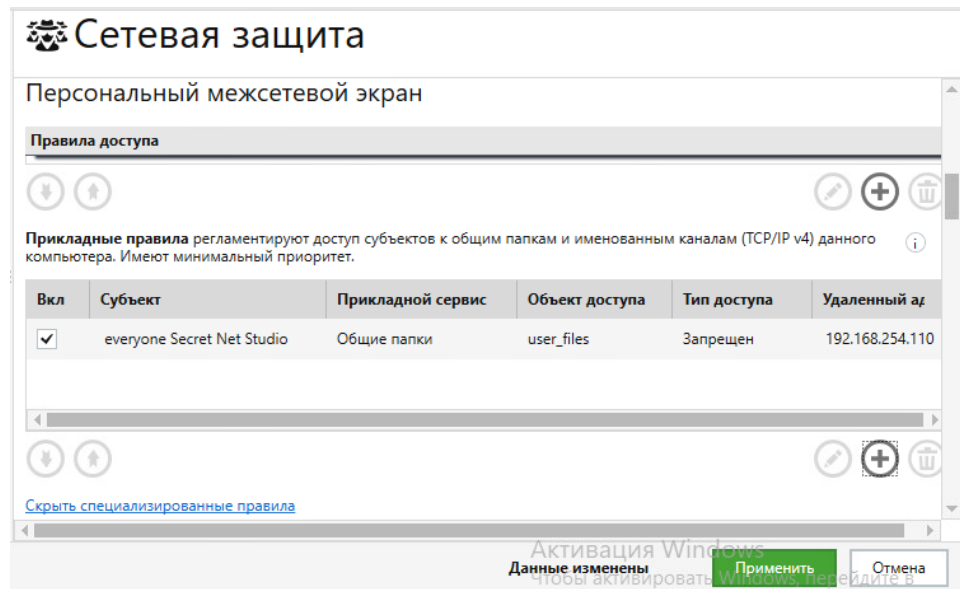
- нажмите кнопку "Далее". На следующем шаге настраиваются дополнительные параметры. В поле "Удаленный адрес" введите **192.168.254.110** – адрес компьютера SNS-Client;

- нажмите кнопку "Далее". На предпоследнем шаге можно настроить расписание. Еще раз нажмите кнопку "Далее" – откроется завершающее окно для создания дополнительного правила доступа;

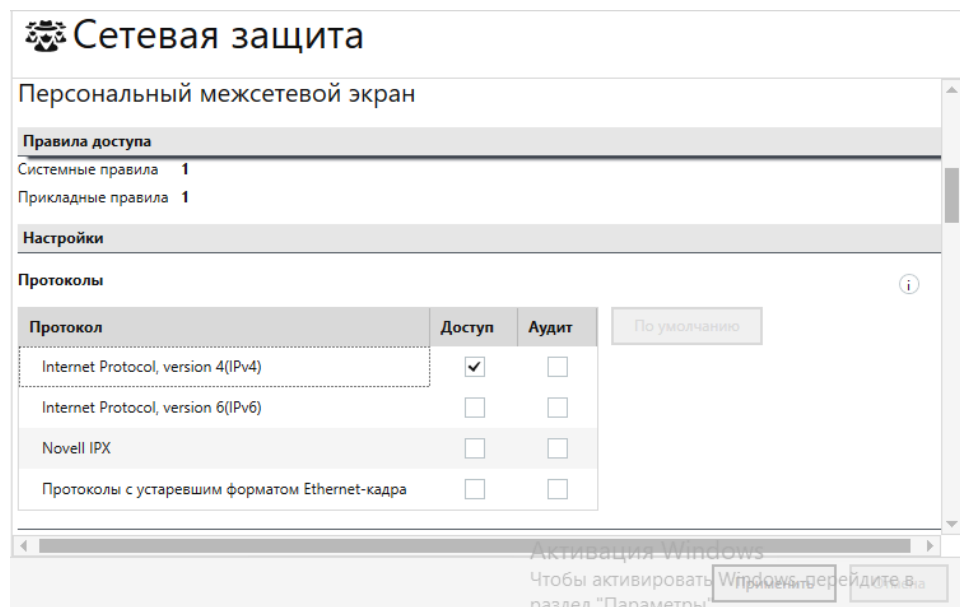
- установите отметку в поле "Создать правило доступа по протоколу SMB", чтобы создать правило доступа, разрешающее прохождение пакетов по протоколу TCP на порт 445 (и/или 139) для учетной записи (или группы), указанной в прикладном правиле. Это требуется, поскольку для корректной работы прикладных правил необходимо настроить правила прохождения IP-пакетов на транспортном уровне – по протоколу SMB;

Внимание! Если прохождение пакетов по протоколу SMB запрещается системными правилами или правилами доступа, то прикладные правила не работают, так как на транспортном уровне IP-пакеты блокируются.

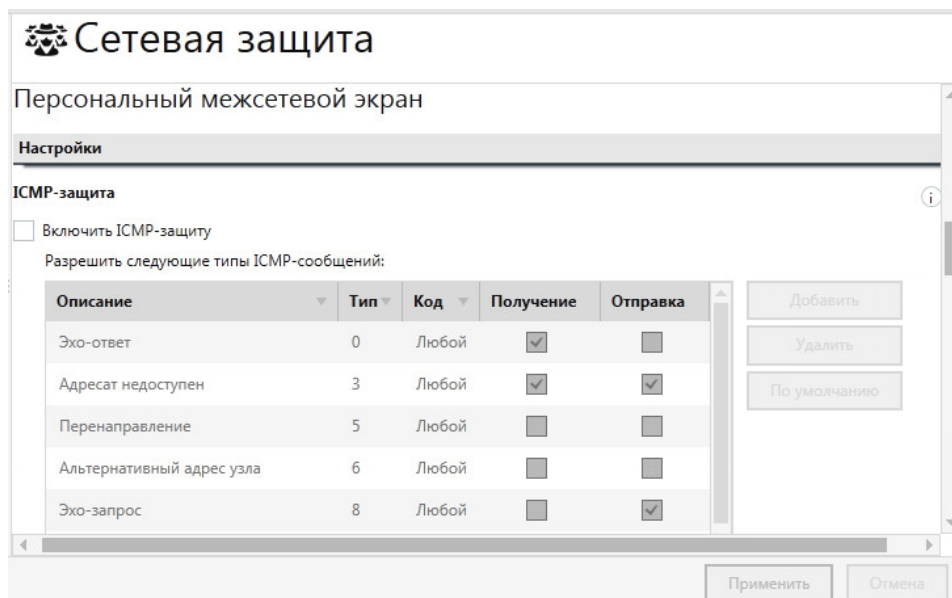
- нажмите кнопку "Готово". В список прикладных правил будет добавлено новое правило. Кроме того, в список правил доступа также будет добавлено дополнительное правило, разрешающее использование SMB для учетной записи (группы), указанной в прикладном правиле.



7. На вкладке "Настройки" нажмите кнопку "Применить". Под таблицей "Прикладные правила" нажмите кнопку-ссылку "Скрыть специализированные правила".
8. В группе настроек "Протоколы" убедитесь, что по умолчанию доступ к защищаемым компьютерам разрешен только по протоколу IPv4. Эти настройки имеют более высокий приоритет, чем все рассмотренные выше правила.



9. Прокрутите список параметров политик персонального межсетевого экрана до группы настроек, которые используются для организации обмена сообщениями по данному протоколу. Обратите внимание, что по умолчанию режим управления пакетами протокола ICMP выключен.

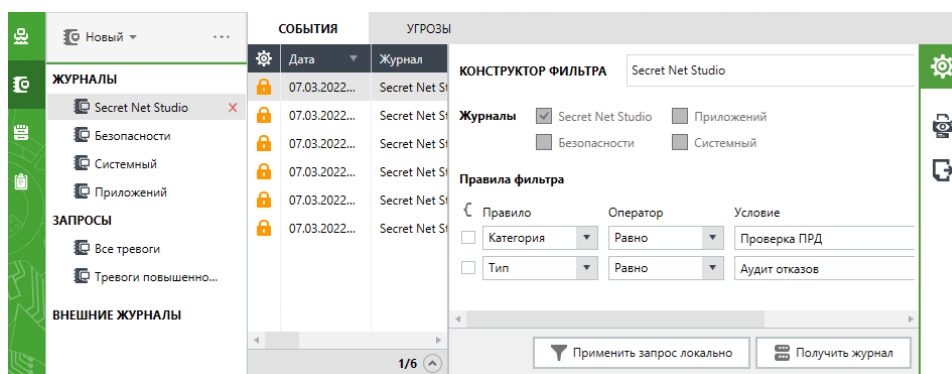


10. Для того чтобы проверить действие политики "ICMP-защита", сделайте следующее:

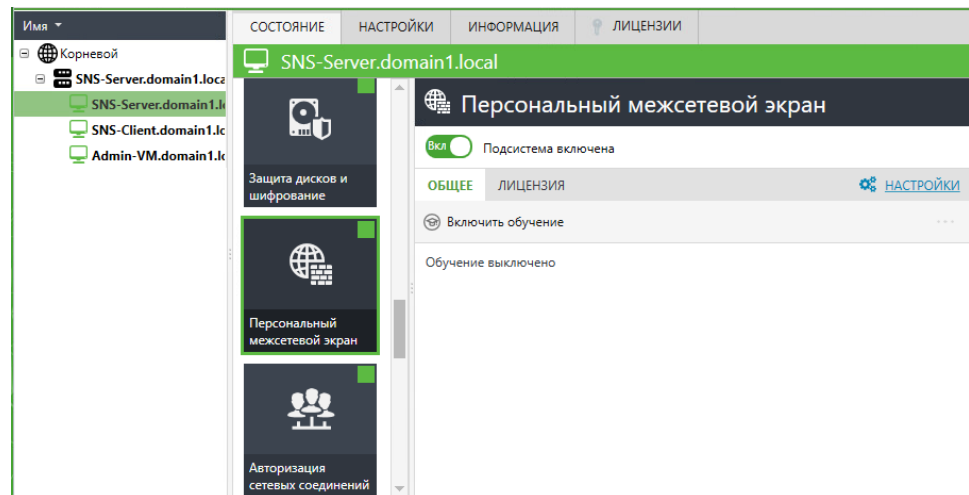
- с VM Admin_VM и SNS_Client последовательно через утилиту "ping" убедитесь, что при выключенной политике "ICMP-защита" доступ по ICMP-протоколу к серверу SNS-Server (192.168.254.20) разрешен;
- включите ICMP-защиту, нажмите кнопку "Применить" и дождитесь появления в панели событий сообщения о сохранении настроек (возможна некоторая задержка в применении политик межсетевого экранирования на агенте);
- повторно используйте ту же команду "ping" и сравните результат.

11. Самостоятельно протестируйте действие созданных ранее правил – запрета RDP-подключения с компьютера SNS-Client к серверу SNS-Server и запрета обращения к общедоступной папке "user_files" с компьютера SNS-Client.

12. Переключитесь в окно BM SNS_Server, откройте программу управления в локальном режиме и в журнале Secret Net Studio просмотрите связанные с работой компонента ПМЭ события категории "Проверка ПРД" с типом "Аудит отказов".



13. Переключитесь в окно BM Admin_VM, в Центре управления откройте панель свойств агента SNS-Server и на вкладке "Состояние" выберите плитку компонента "Персональный межсетевой экран".



Обратите внимание, что данная вкладка позволяет включать/отключать на защищаемом компьютере работу данного компонента, а также управлять работой режима обучения. Кроме того, с помощью кнопки-ссылки "Перейти к настройке подсистемы" можно перейти к настройке политик межсетевого экрана, с которыми мы познакомились в данном сценарии.

Выполнение сценария завершено.

Сценарий №11 "Авторизация сетевых соединений"

В данном сценарии рассматриваются некоторые примеры применения механизма авторизации сетевых соединений для обеспечения защищенного взаимодействия между авторизованными на сервере безопасности Secret Net Studio абонентами (пользователями и компьютерами).

Для установления защищенного соединения необходимо:

- настроить для удаленного компьютера-получателя правила доступа, необходимые для обмена данными с компьютером-отправителем (авторизация сетевых соединений работает в непосредственном взаимодействии с правилами межсетевого экранирования);
- включить режим подписи или шифрования IP-пакетов на компьютере-отправителе.

При невыполнении одного из этих условий установить защищенное соединение невозможно.

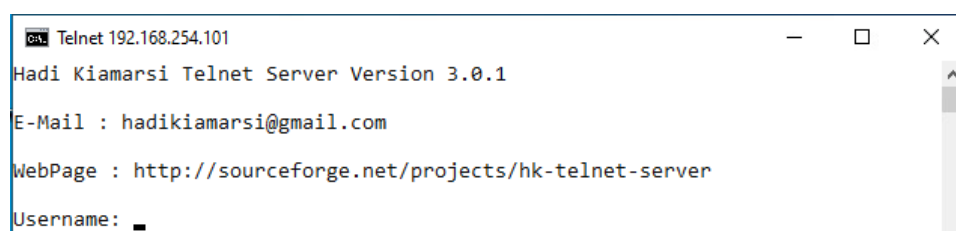
Настройка механизма авторизации сетевых соединений осуществляется централизованно в программе "Центр управления". Программа управления в локальном режиме непосредственно на защищаемом компьютере позволяет только просматривать централизованно заданные параметры.

Внимание! Перед началом выполнения сценария включите BM Sniffer и убедитесь, что на ней установлена программа Wireshark и сетевой интерфейс подключен к порт-группе, работающей в режиме Promiscuous mode.

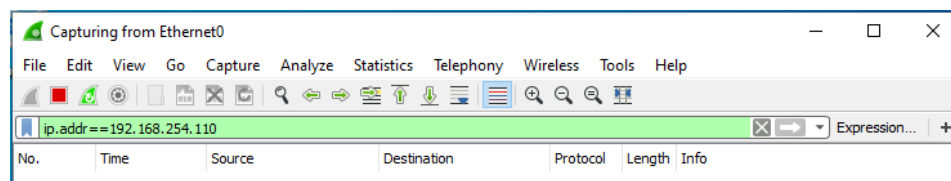
1. На VM Admin_VM в Центре управления отключите все заданные в предыдущем сценарии запрещающие правила и примените настройки.
2. Убедитесь, что при выключенном механизме авторизации сетевых соединений между клиентами Secret Net Studio передается открытый трафик. Для этого:
 - на VM Admin_VM из папки "C:\Distrib\hk-telnet-server-3-0-1" запустите утилиту telnet-сервера "hk-telnet-server" и в открывшемся окне нажмите кнопку "START";



- переключитесь в окно BM SNS_Client, откройте от имени администратора командную строку и начните подключение по telnet к BM Admin_VM: **telnet 192.168.254.101**. В окне telnet-сессии появится приглашение для ввода учетных данных;



- переключитесь в окно BM Sniffer, запустите утилиту Wireshark и начните перехват трафика, указав в поле "Apply a display filter" строку фильтра **ip.addr==192.168.254.110**;



- переключитесь на BM SNS_Client и на запрос учетных данных для telnet-сессии последовательно введите: username – **admin**, Password – **P@ssw0rd** (при вводе каждый символ удваивается!). После авторизации на telnet-сервере введите команду **hostname**, чтобы убедиться в успешном подключении к Admin-VM;

```

Username: aaddmiiinn
Password: P*@*s*s*w*0*r*d*

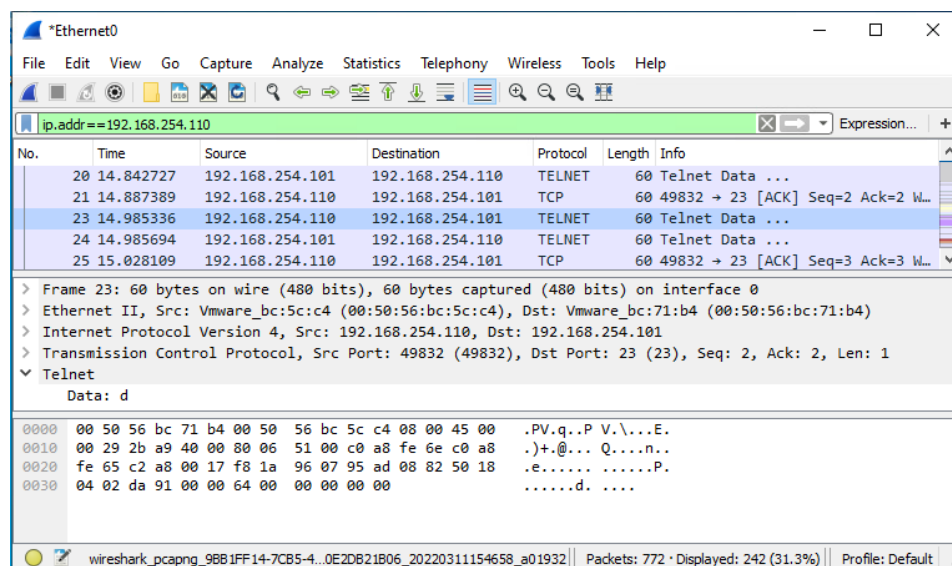
[ USERNAME = admin ] YOUR IP ADDRESS : 192.168.254.110
Welcome to Hadi Kiamarsi TELNET Server.

TELNET # C:\Distrib\hk-telnet-server-3-0-1>hostname
Admin-VM

TELNET # C:\Distrib\hk-telnet-server-3-0-1>_

```

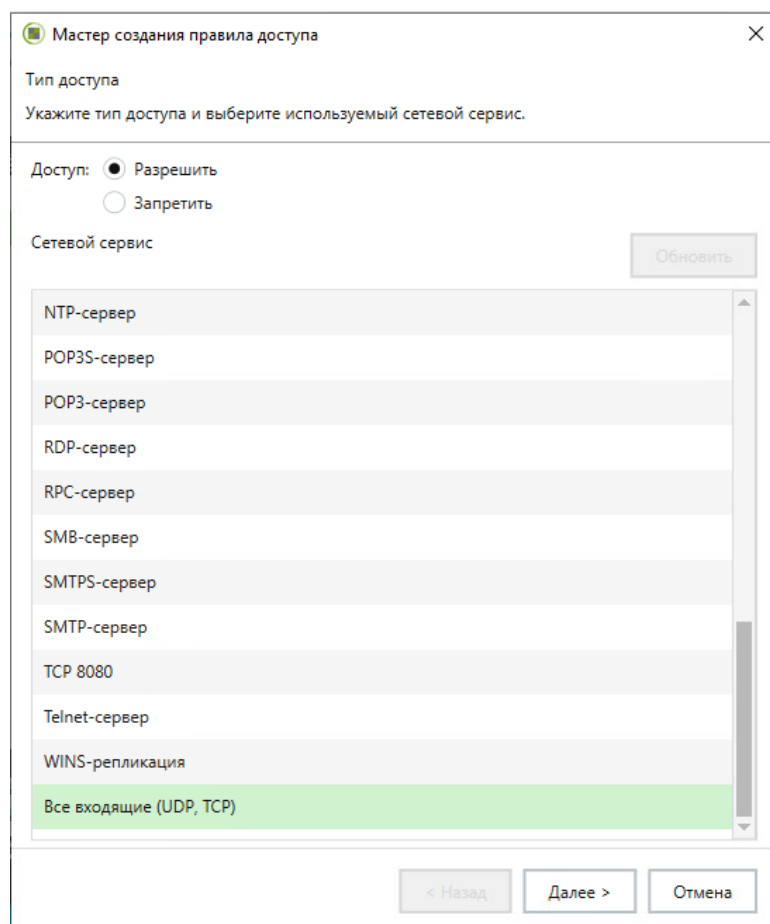
- переключитесь в окно BM Sniffer, в окне Wireshark остановите перехват трафика, найдите записи протокола telnet и убедитесь, что при вводе логина и пароля от источника (192.168.254.110) к получателю (192.168.254.101) символы передавались открытым текстом.



Таким образом, можно констатировать, что при отключенном механизме авторизации сетевых соединений между клиентами Secret Net Studio передается незащищенный трафик.

3. Перед установлением защищенного соединения для взаимодействия между компьютерами отправителя и получателя на VM Admin_VM в панели "Компьютеры" программы управления выберите объект Admin_VM и, используя описание пп. 1, 2 предыдущего сценария, создайте для абонентов группы "Everyone" разрешающее правило доступа для TCP /UDP-трафика на любой порт с любого удаленного порта.

Пользователь	Источник	Протокол/порт	Получатель	Протокол/порт	Действие
everyone	*	TCP, UDP / any	*	any / any	allow



Мастер создания правила доступа

Параметры правила
Укажите тип протокола, направление соединения, удаленный порт и приложение, для которого будет действовать правило.

Тип протокола: TCP, UDP

Направление: ☒ Входящее
☐ Исходящее
☐ Требовать защищенное соединение

Порт назначения: * Дополнительно

Приложение: *

< Назад Далее > Отмена

Мастер создания правила доступа

Субъект доступа
Выберите учетную запись или группу, доступ которой будет контролировать создаваемое правило.

Субъект доступа: everyone Secret Net Studio Выбрать

< Назад Далее > Отмена

Мастер создания правила доступа

Настройка уведомлений
Укажите способы сигнализации о срабатывании правила.

При наступлении события:

☒ Включить аудит

☐ Звуковая сигнализация

☐ Выполнить команду

в пользовательской сессии: Системной

☐ Запустить с повышенными правами

< Назад Далее > Отмена

Мастер создания правила доступа

Дополнительные критерии

Укажите дополнительные параметры правила, такие как адреса узлов и маска фильтра.

Маска фильтра:

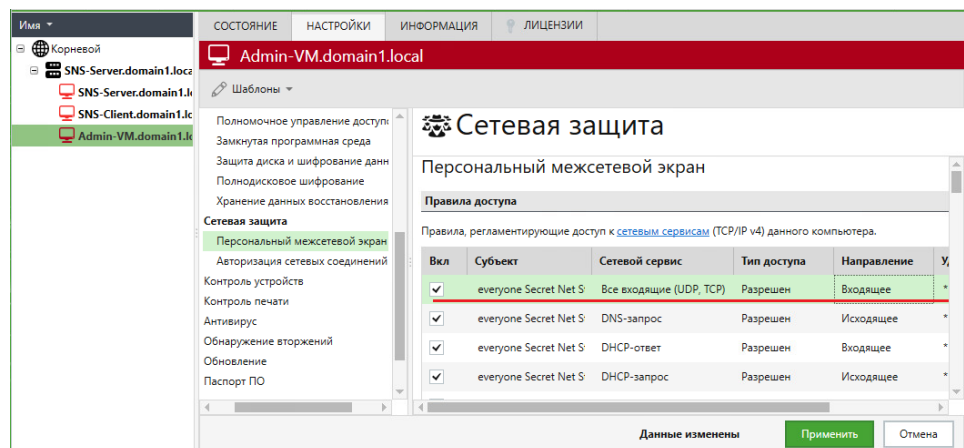
Удаленный адрес:

Локальный адрес:

☐ Отключить правило

☒ Уведомлять отправителя о блокировке пакета

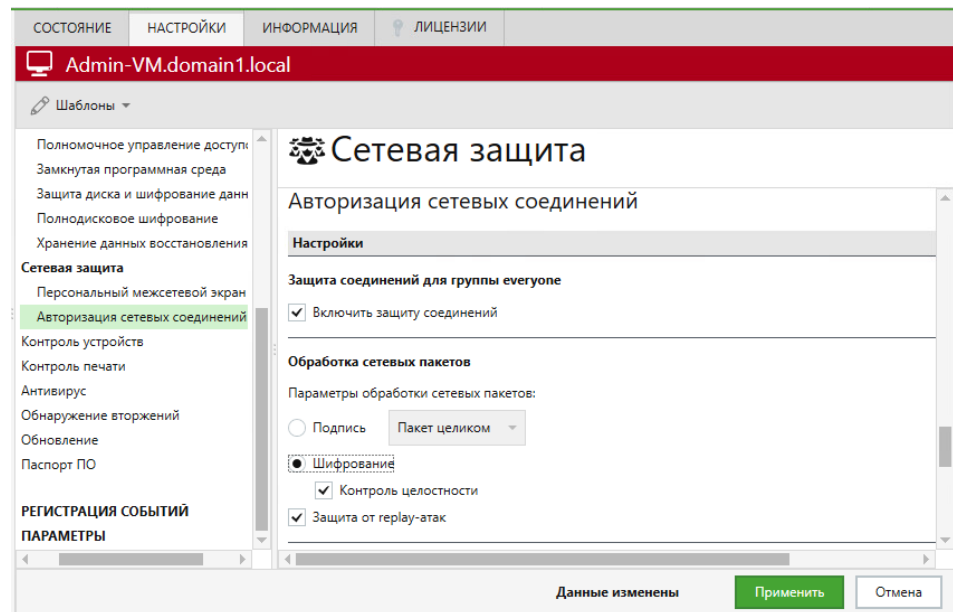
< Назад Далее > Отмена



Примечание. Группа Everyone включает в себя пользователей и компьютеры, которые:

- прошли аутентификацию на СБ Secret Net Studio (authenticated Secret Net Studio), т.е. с установленным клиентом SNS;
- не прошли аутентификацию на СБ SNS (anonymous), т.е. либо не установлен клиент SNS, либо имеется проблема сетевого взаимодействия между клиентом и СБ.

4. Настройте режим защиты сетевых соединений между авторизованными клиентами Secret Net Studio. Для этого:
 - для объекта Admin_VM на вкладке "Настройки" выберите раздел "Политики / Сетевая защита / Авторизация сетевых соединений";
 - в группе настроек "Защита соединений для группы everyone" установите отметку в поле "Включить защиту соединений";
 - в группе настроек "Обработка сетевых пакетов" установите отметку в поле "Шифрование" и убедитесь, что отмечены опции "Контроль целостности" и "Защита от replay-атак";
 - остальные параметры оставьте заданными по умолчанию. Примените сделанные настройки и убедитесь, что в панели событий появилась запись об успешном сохранении конфигурации.

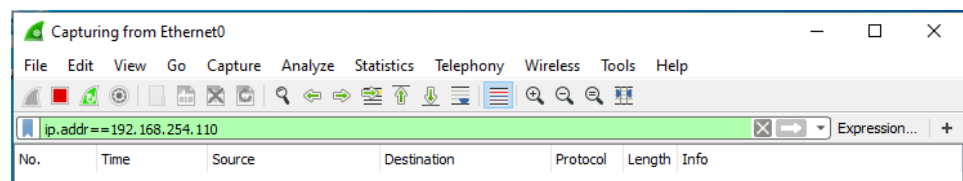


5. Убедитесь, что после включения механизма авторизации сетевых соединений между клиентами Secret Net Studio передается защищенный трафик. Для этого:

- на BM SNS_Client закройте открытое ранее telnet-подключение к Admin-VM, используя команду **exit**;
- начните новое telnet-подключение к Admin-VM: **telnet 192.168.254.101**. В окне telnet-сессии появится приглашение для ввода учетных данных;

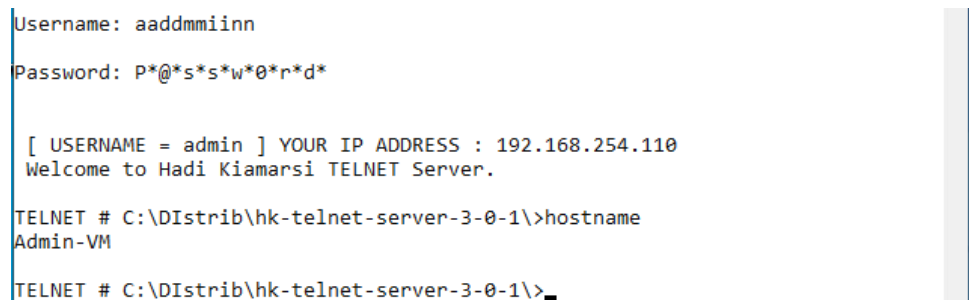


- переключитесь в окно BM Sniffer и в программе Wireshark снова начните перехват трафика с тем же фильтром в строке "Apply a display filter" – **ip.addr==192.168.254.110**;

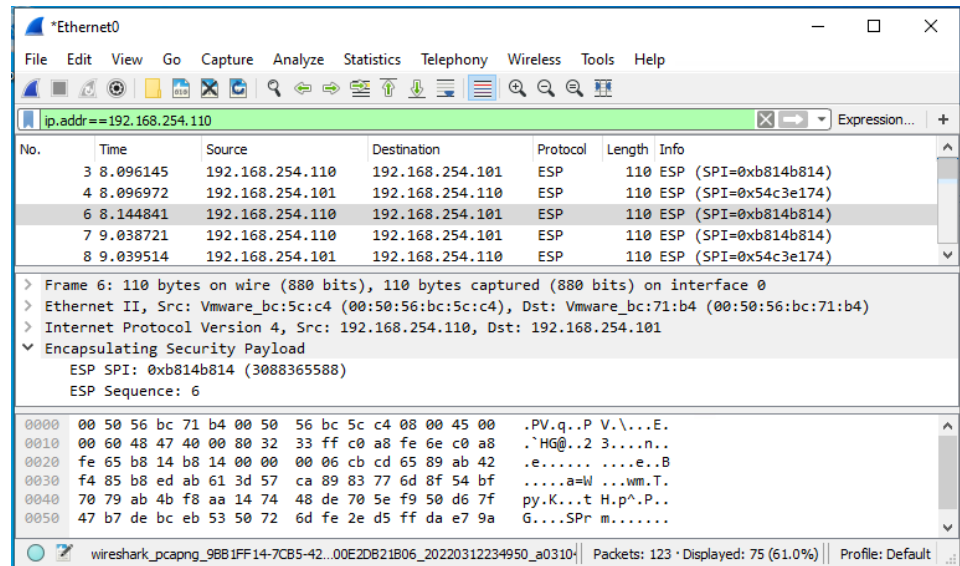


- переключитесь на BM SNS_Client и на запрос учетных данных для telnet-сессии последовательно введите: username – **admin**, Password – **P@ssw0rd** (при вводе каждый символ удваивается!).

После авторизации на telnet-сервере введите команду **hostname**, чтобы убедиться в успешном подключении к Admin-VM;



- переключитесь в окно BM Sniffer, в утилите Wireshark остановите перехват трафика и убедитесь, что после включения защиты соединений от источника (192.168.254.110) к получателю (192.168.254.101) вместо открытого протокола telnet передаются пакеты по ESP-протоколу, который не содержит открытых (незашифрованных) данных.



Таким образом, можно констатировать, что при включенном механизме авторизации сетевых соединений между клиентами Secret Net Studio передается защищенный трафик, который не содержит открытой информации.

6. Переключитесь на BM SNS_Client и закройте открытое ранее подключение по telnet к Admin-VM, используя команду **exit**.

Переключитесь в окно BM Admin_VM и завершите работу telnet-сервера "hk-telnet-server".

Аналогичный подход может применяться для обеспечения безопасности не только telnet-подключений, но и других используемых сетевых сервисов, которые передают информацию в открытом виде, например, http (обеспечение безопасного подключения клиентов к развернутому в организации веб-серверу).

7. Как уже отмечалось выше, механизм авторизации сетевых соединений обеспечивает защиту взаимодействия только между авторизованными на СБ клиентами Secret Net Studio. Если на компьютере пользователя не установлен агент Secret Net Studio или пользователь по каким-либо причинам не прошел аутентификацию на СБ SNS (anonymous), то трафик между ним и авторизованным клиентом SNS не будет защищаться.

Однако с помощью соответствующих правил межсетевого экранирования администратор может настроить блокировку соединений для неавторизованных на СБ пользователей (anonymous). Для этого:

- в окне программы управления на BM Admin_VM в панели "Компьютеры" для объекта Admin-VM на вкладке "Настройки" выберите раздел "Политики / Сетевая защита / Персональный межсетевой экран";
- используя описание пп. 1, 2 предыдущего сценария и п. 3, создайте для клиентов группы anonymous запрещающее правило доступа для входящего TCP /UDP-трафика на любой порт с любого удаленного порта.

Пользователь	Источник	Протокол/порт	Получатель	Протокол/порт	Действие
anonymous	*	TCP, UDP / any	*	any / any	deny

Мастер создания правила доступа

Тип доступа
Укажите тип доступа и выберите используемый сетевой сервис.

Доступ: ☐ Разрешить
☒ Запретить

Сетевой сервис

Обновить

NTP-сервер

POP3S-сервер

POP3-сервер

RDP-сервер

RPC-сервер

SMB-сервер

SMTPS-сервер

SMTP-сервер

TCP 8080

Telnet-сервер

WINS-репликация

Все входящие (UDP, TCP)

< Назад

Далее >

Отмена

Мастер создания правила доступа

Субъект доступа
Выберите учетную запись или группу, доступ которой будет контролировать создаваемое правило.

Субъект доступа:

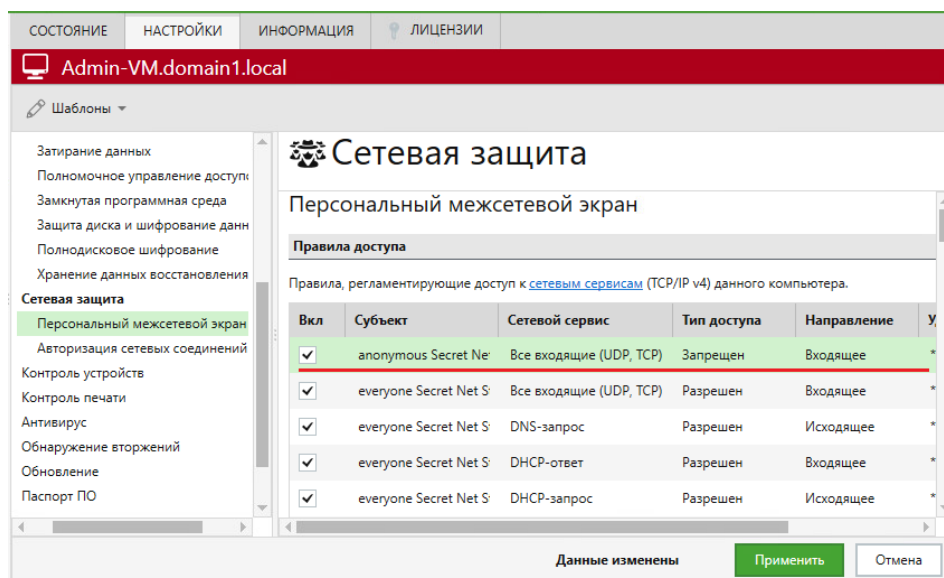
anonymous Secret Net Studio

Выбрать

< Назад

Далее >

Отмена



После применения сделанных изменений сетевое взаимодействие с Admin-VM будет возможным только для авторизованных на СБ абонентов.

Если распространить данный подход на всю сетевую инфраструктуру, весь трафик будет изолирован только между клиентами Secret Net Studio.

8. Выключите BM Sniffer.

На BM Admin_VM в программе управления для объекта Admin-VM отключите режим защиты сетевых соединений (см. п. 4), а также все созданные запрещающие правила и примените изменения.

Выполнение сценария завершено.

Сценарий №12 "Настройка антивируса и COB"

Настройка параметров антивируса и COB осуществляется администратором безопасности с помощью групповых и локальных политик в программе управления Secret Net Studio.

В данном сценарии показываются некоторые способы настройки и применения антивируса и COB.

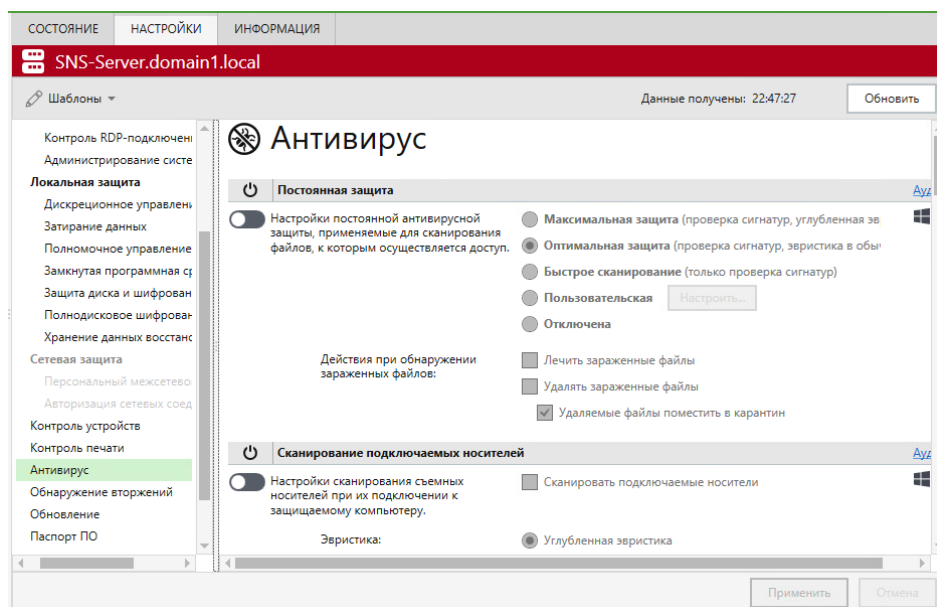
Внимание! Перед началом выполнения данного сценария выполните следующие действия:

- на BM Admin_VM в программе "Центр управления" на вкладке "Состояние" свойств объекта Admin-VM выключите компонент "Персональный межсетевой экран";
- на BM SNS-Client под учетной записью "snsadmin" для проведения атак последовательно установите из папки "C:\Distrib\sniff_utils" следующее ПО: "WinPcap 4.1.3", "ettercap-NG-0.7.3-win32" и "nmap 7.1.2".

1. Ознакомьтесь с параметрами настройки групповых политик антивируса на уровне сервера безопасности. Для этого:

- на BM Admin_VM в программе "Центр управления" выберите объект сервера подключения SNS-Server и в панели его свойств на вкладке "Настройки" выберите раздел "Политики / Антивирус". В рабочей области окна появятся параметры настройки групповых политик;

В случае необходимости управления локальными настройками антивируса на защищаемом компьютере нужно выбрать соответствующий объект в программе управления.

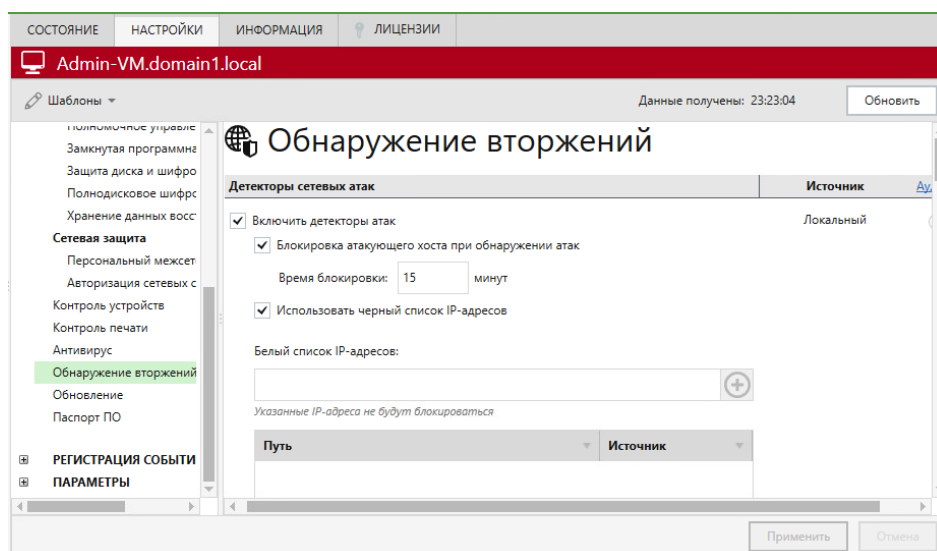


- обратите внимание, что первым располагается профиль "Постоянная защита", который определяет параметры сканирования объектов системы в режиме реального времени.

С помощью кнопки  ознакомьтесь с описанием профиля "Постоянная защита". Обратите внимание, что если одновременно отмечены пункты "Лечить зараженные файлы" и "Удалять зараженные файлы", то при обнаружении зараженных объектов сначала будет выполнена попытка их лечения, а затем, при неудаче, файлы будут удалены.

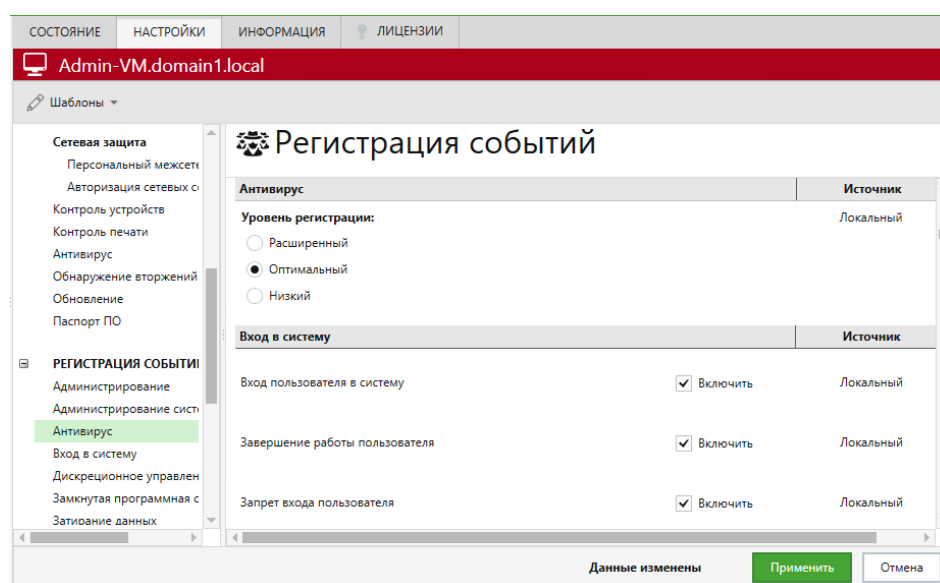
Эвристический анализатор ищет фрагменты кода и программы, имеющие вирусоподобные характеристики, но не зарегистрированные в БД вирусных сигнатур. При обнаружении такого подозрительного файла выполняется оповещение пользователя. В выбранном по умолчанию профиле "Оптимальная защита" используется "Обычный режим" анализатора — глубина эвристики ограничена, низкая вероятность ложных срабатываний, но и вероятность обнаружения неизвестных вирусов не слишком высока. При выборе профиля "Максимальная защита" эвристический анализатор будет работать в режиме "Углубленная эвристика" — высокая вероятность обнаружения неизвестных вирусов, однако и выше вероятность ложных срабатываний.

2. Проведите настройку политик COB на клиенте SNS, установленном на компьютере администратора. Для этого в программе управления в сетевом режиме выберите в панели "Компьютеры" объект Admin-VM, в панели его свойств на вкладке "Настройки" выберите раздел "Политики / Обнаружение вторжений" и установите следующие параметры политик:



- "Включить детекторы атак" – убедитесь, что установлен флажок;

- "Блокировка атакующего хоста..." – оставьте отмеченным, "Время блокировки" – **3** минуты;
- "Использовать черный список IP-адресов" – оставьте отмеченным (параметр по умолчанию активен для всех детекторов). В этом случае будут заблокированы вредоносные IP-адреса из базы опасных веб-ресурсов Kaspersky;
- "Белый список IP-адресов" – оставьте пустым. В это поле можно ввести IP-адреса (например, 192.168.100.25) или маску подсети в нотации CIDR (например, 192.168.100.0/24), которые не будут блокироваться детекторами атак;
- ниже, в группе "Детекторы", установите отметку в поле "Сканирование портов". В параметрах "Период обнаружения" и "Максимальное количество обращений к портам" оставьте значения по умолчанию;
- выберите раздел "Регистрация событий / Антивирус" и убедитесь, что установлен уровень "Оптимальный", при котором регистрируются все важные и некоторые информационные события. Если выбрать опцию "Расширенный", то будут регистрироваться все происходящие события, и их количество может оказаться очень большим;



- выберите раздел "Регистрация событий / Обнаружение вторжений" и просмотрите заданный по умолчанию перечень регистрируемых событий данной подсистемы;
 - нажмите кнопку "Применить" и убедитесь, что в панели событий появилось соответствующее сообщение о сохранении настроек.
3. Переключитесь в консоль BM SNS_Client и симулируйте атаку на компьютер Admin-VM. Для этого:
- откройте от имени администратора командную строку и через утилиту **ping** убедитесь, что компьютер Admin-VM (192.168.254.101) доступен;
 - откройте от имени администратора еще одно окно командной строки и проведите сканирование портов защищаемого компьютера с помощью команды **nmap -T5 -PN 192.168.254.101**;

```

Командная строка

C:\Users\snsadmin>nmap -T5 -PN 192.168.254.101

Starting Nmap 7.12 ( https://nmap.org ) at 2022-03-15 21:19 RTZ 2 (ceia)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.254.101
Host is up (0.019s latency).
Not shown: 800 filtered ports, 197 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:50:56:BC:71:B4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 82.24 seconds
C:\Users\snsadmin>

```

- с помощью утилиты **ping** повторно проверьте доступность компьютера Admin-VM (192.168.254.101) и убедитесь, что эхо-ответы не приходят.

```

Администратор: Командная строка

C:\Windows\system32>ping 192.168.254.101

Обмен пакетами с 192.168.254.101 по 32 байтами данных:
Ответ от 192.168.254.101: число байт=32 время=1мс TTL=128
Ответ от 192.168.254.101: число байт=32 время=1мс TTL=128
Ответ от 192.168.254.101: число байт=32 время=1мс TTL=128
Ответ от 192.168.254.101: число байт=32 время=1мс TTL=128

Статистика Ping для 192.168.254.101:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек

C:\Windows\system32>ping 192.168.254.101

Обмен пакетами с 192.168.254.101 по 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 192.168.254.101:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (100% потерь)

C:\Windows\system32>

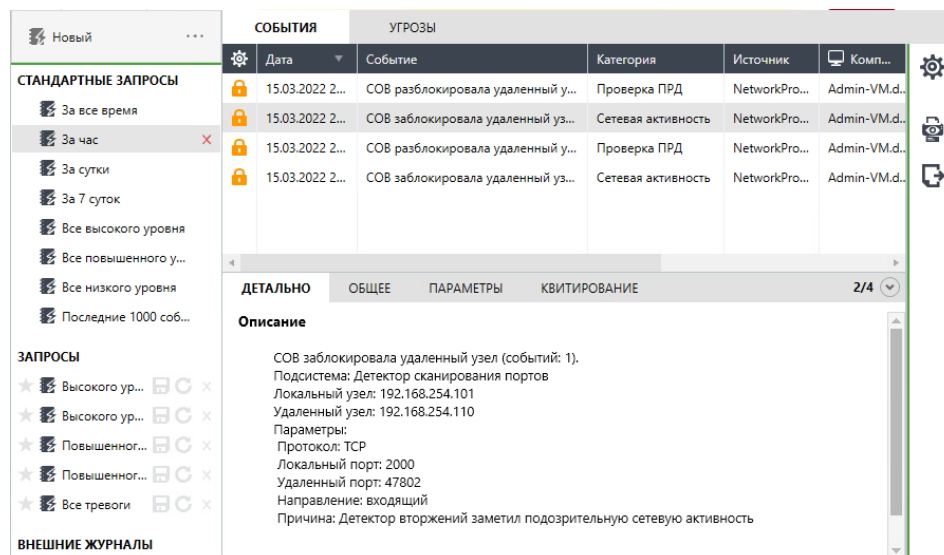
```

4. Переключитесь в консоль VM Admin_VM и убедитесь, что:

- в панели событий появились записи о событиях тревоги на Admin-VM;

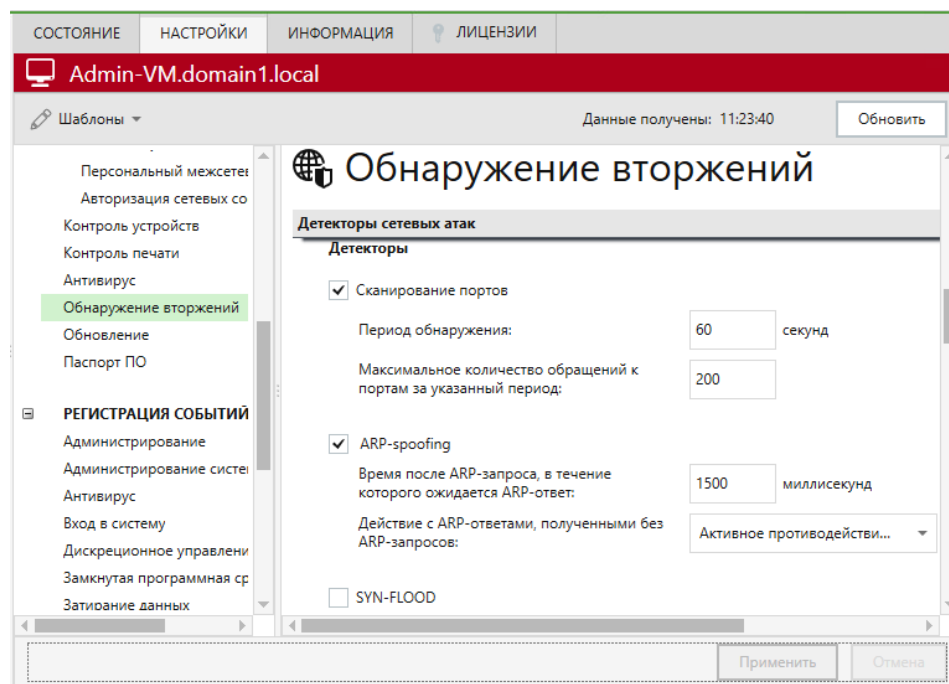
Тип	Дата и время	Событие	Описание
	15.03.2022 21:29:36	Тревоги на станции. Компьютер: Admin-VM.domain1.local. Тревоги: 1(1).	Получить описание тревоги.
	15.03.2022 21:26:21	Тревоги на станции. Компьютер: Admin-VM.domain1.local. Тревоги: 1(1).	Получить описание тревоги.
	15.03.2022 21:22:55	Тревоги на станции. Компьютер: Admin-VM.domain1.local. Тревоги: 1(1).	Получить описание тревоги.
	15.03.2022 21:20:15	Тревоги на станции. Компьютер: Admin-VM.domain1.local. Тревоги: 1(1).	Получить описание тревоги.

- в журнале тревог появились сообщения о блокировке атакующего узла категории "Сетевая активность" с типом "Аудит отказов", а также сообщения с категорией "Проверка ПРД" о разблокировании удаленного компьютера. Обратите внимание, что детальная информация о событиях блокировки содержит сведения о сетевом протоколе и об удаленном и локальном портах, по которым проводилось сканирование.



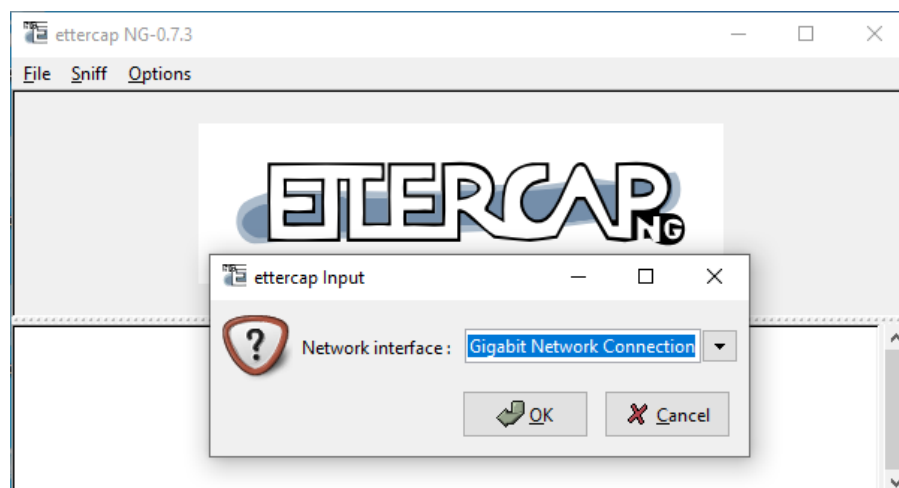
5. Проведите дополнительную настройку политик COV на клиенте Admin-VM. Для этого в панели его свойств на вкладке "Настройки" выберите раздел "Политики / Обнаружение вторжений" и установите следующие параметры:

- в группе "Детекторы" установите отметку в поле "ARP-spoofing";
- параметры: "Время после ARP-запроса..." – 1500мс. (по умолчанию), "Действие с ARP-ответами..." – "Активное противодействие" (по умолчанию);
- нажмите кнопку "Применить" и дождитесь применения политик на агенте и появления в панели событий соответствующего сообщения.

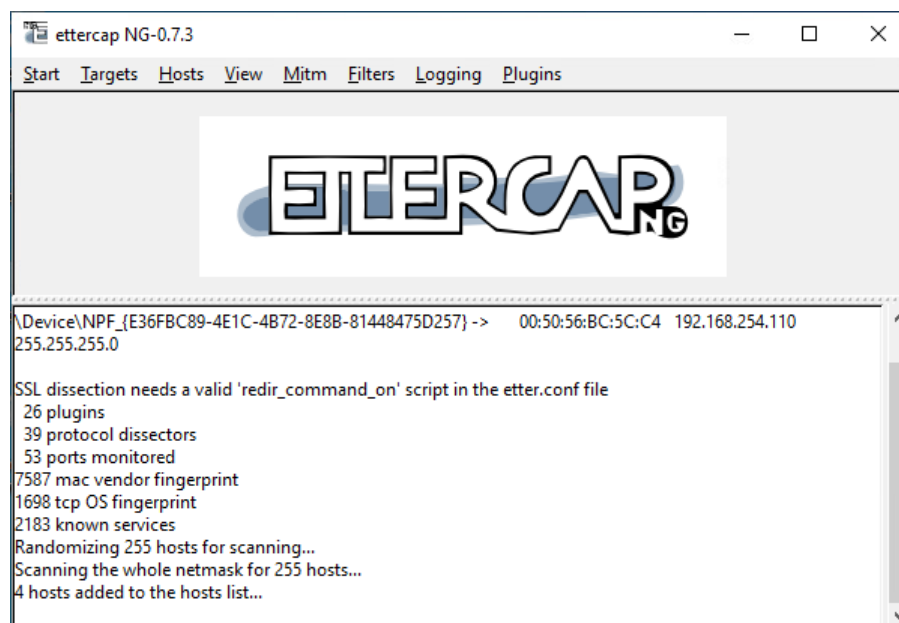


6. Сымитируйте атаку ARP-spoofing на компьютер Admin_VM. Для этого:

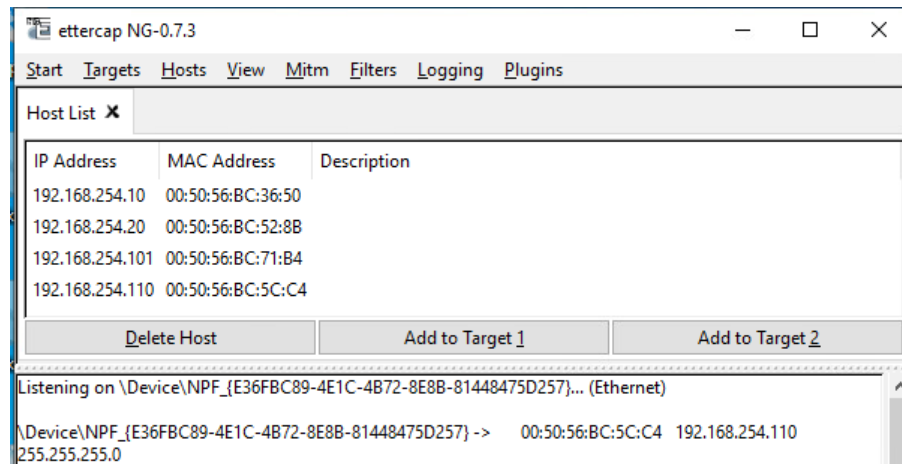
- в окне BM Admin_VM с помощью утилиты **arp -a** определите и запишите MAC-адрес компьютера SNS-Server (192.168.254.20): _____;
- в окне консоли Admin_VM запустите постоянную проверку доступности компьютера SNS-Server командой **ping -t 192.168.254.20**;
- переключитесь в консоль BM SNS_Client и запустите Ettercap NG-0.7.3. В открывшемся окне программы в главном меню выберите опцию "Sniff / Unified sniffing...";



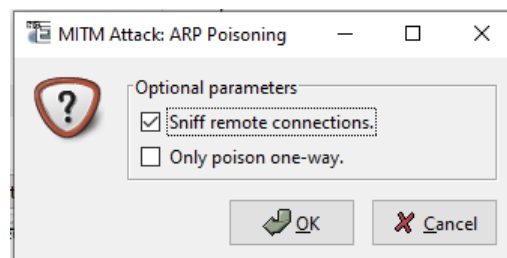
- в открывшемся диалоговом окне убедитесь, что в раскрывающемся списке выбран сетевой интерфейс и нажмите кнопку "OK". Обратите внимание, что в нижней части окна "Ettercap NG-0.7.3" появилось описание параметров выбранного интерфейса компьютера SNS-Client;
- в окне "Ettercap NG-0.7.3" в главном меню выберите опцию "Hosts / Scan for hosts". Дождитесь завершения сканирования доступных хостов в сети. В нижней части окна появятся сообщения об обнаруженных хостах и добавлении доступных хостов в список;



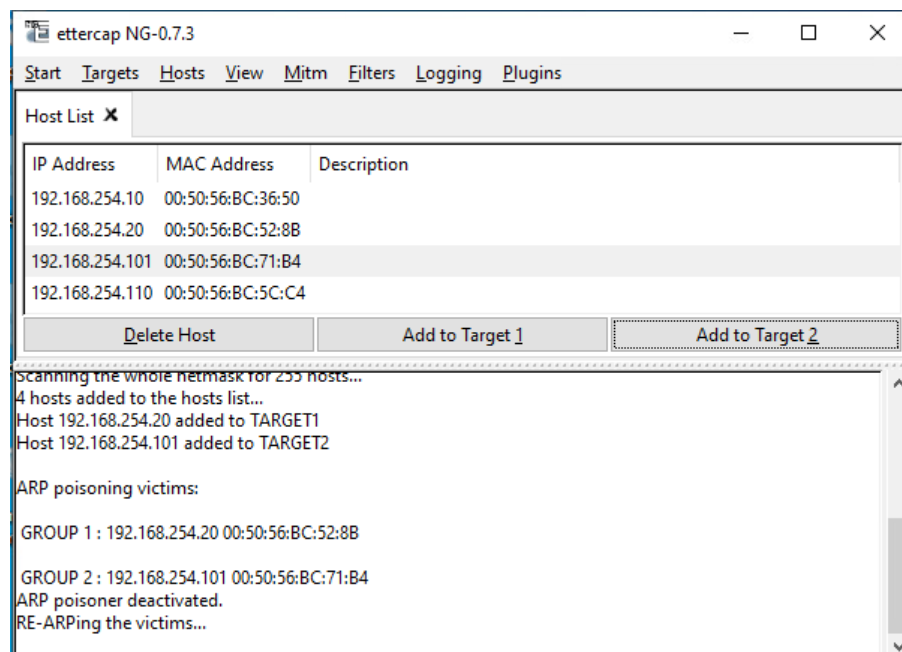
- в главном меню окна "Ettercap NG-0.7.3" выберите опцию "Hosts / Host list". В верхней части окна вы увидите список доступных хостов в сети;



- выберите хост 192.168.254.20 (компьютер SNS-Server) и нажмите кнопку "Add to Target 1", а затем выберите атакуемый компьютер 192.168.254.101 (компьютер Admin_VM) и нажмите кнопку "Add to Target 2". В нижней части окна появятся записи по заданным целям;
- запустите атаку ARP-spoofing. Для этого из главного меню выберите опцию "Mitm / ARP poisoning...", в открывшемся диалоговом окне отметьте опцию "Sniff remote connections" и нажмите кнопку "OK";



- перейдите в окно консоли Admin_VM и с помощью утилиты **arp -a** определите MAC-адрес компьютера SNS-Server (192.168.254.20). Убедитесь, что он совпадает с тем, что вы записывали в начале теста. Атака была заблокирована системой защиты Secret Net Studio;
- в окне SNS-Client остановите атаку, выбрав опцию "Mitm / Stop mitm attack(s)". В нижней части окна появится соответствующее сообщение.



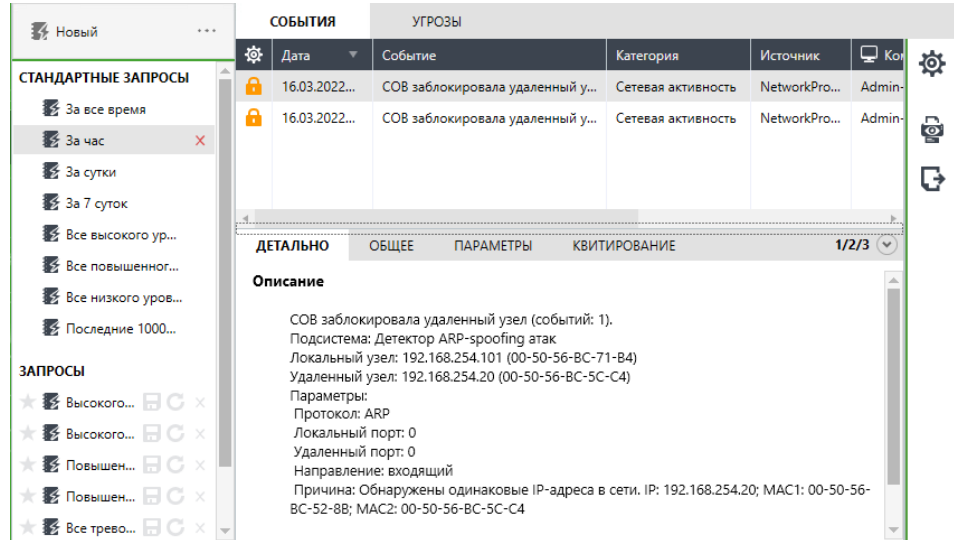
7. Переключитесь в окно консоли Admin_VM и остановите проверку доступности компьютера SNS-Server командой **ping**;

8 Откройте окно программы управления и убедитесь, что:

- в панели событий появились записи о событиях тревоги на Admin-VM;

Тип	Дата и время	Событие	Описание	89/1244
	16.03.2022 13:32:59	Тревоги на станции. Компьютер: Admin-VM.domain1.local. Тревоги: 1(1).	Получить описание тревоги.	
	16.03.2022 13:32:49	Тревоги на станции. Компьютер: Admin-VM.domain1.local. Тревоги: 1(1).	Получить описание тревоги.	

- в журнале тревог  появились сообщения детектора атак об арг-спуфинге (категория – "Сетевая активность", тип – "Аудит отказов").



The screenshot shows a security management interface with a left sidebar containing filters and a main panel displaying event logs. The event log table has columns: Дата, Событие, Категория, Источник, and Кол. Two events are listed, both with the category 'Сетевая активность' and source 'NetworkPro...'. The details pane for the selected event shows the following information:

Описание

СОВ заблокировала удаленный узел (событий: 1).
 Подсистема: Детектор ARP-spoofing атак
 Локальный узел: 192.168.254.101 (00-50-56-BC-71-B4)
 Удаленный узел: 192.168.254.20 (00-50-56-BC-5C-C4)
 Параметры:
 Протокол: ARP
 Локальный порт: 0
 Удаленный порт: 0
 Направление: входящий
 Причина: Обнаружены одинаковые IP-адреса в сети. IP: 192.168.254.20; MAC1: 00-50-56-BC-52-8B; MAC2: 00-50-56-BC-5C-C4

Выполнение сценария завершено.