

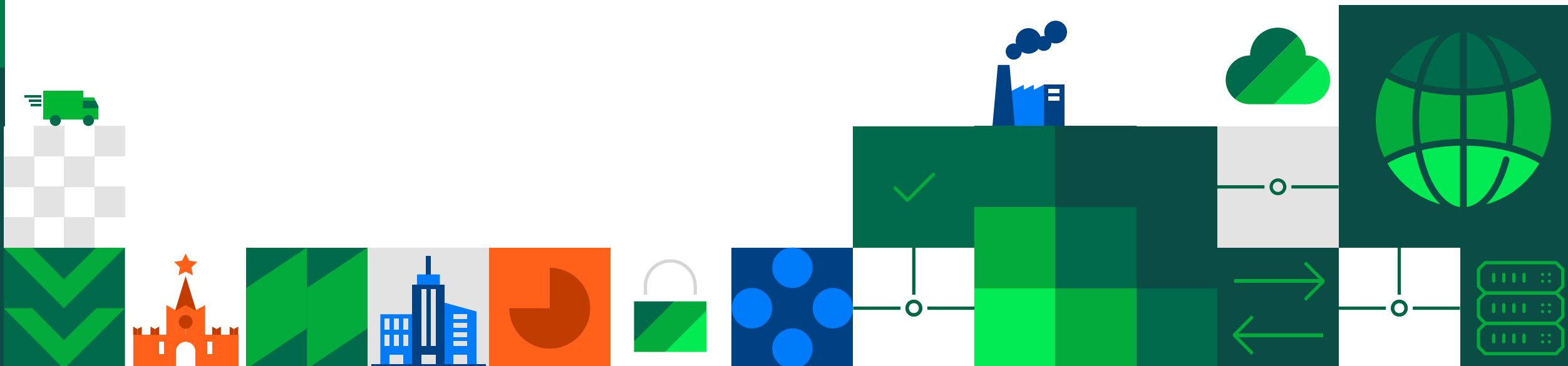


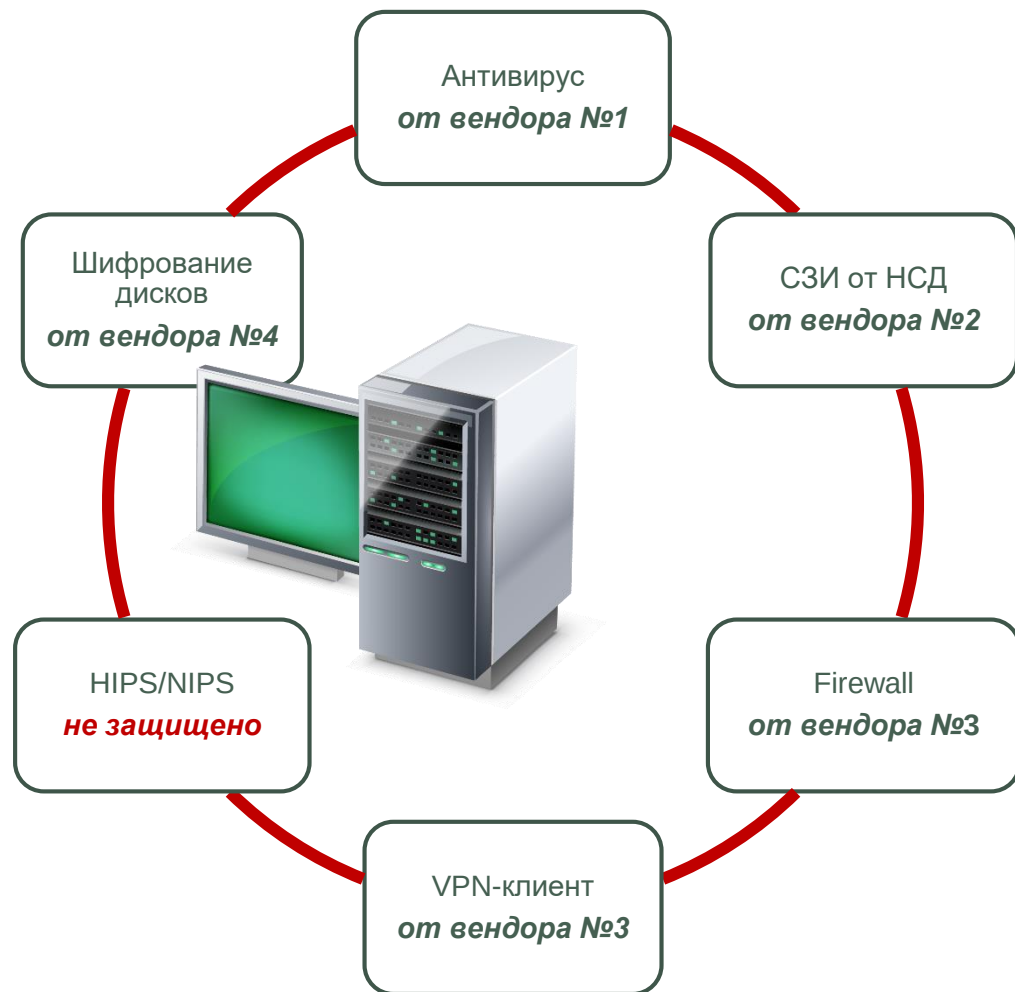
**КОД**  
безопасности



# Применение системы защиты Secret Net Studio

---





## Трудности многовендорной защиты:

Несогласованная работа защитных подсистем – конфликты в работе СЗИ и снижение общего уровня ИБ

Отсутствие ответственности вендоров по решению проблем совместимости продуктов

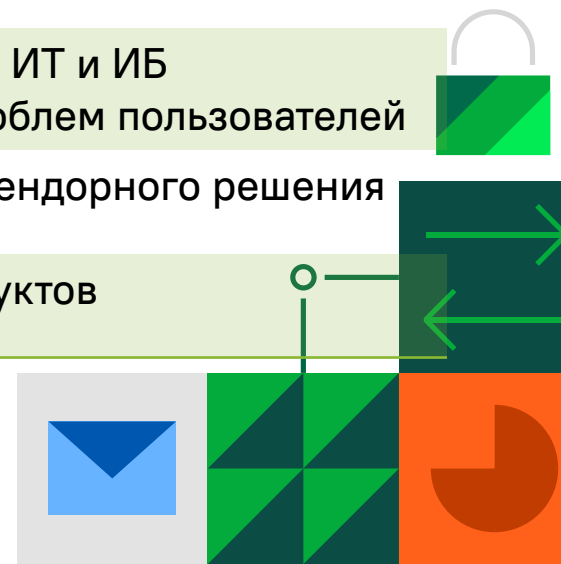
Высокая нагрузка на защищаемые компьютеры ввиду избыточности собираемой разными СЗИ информации

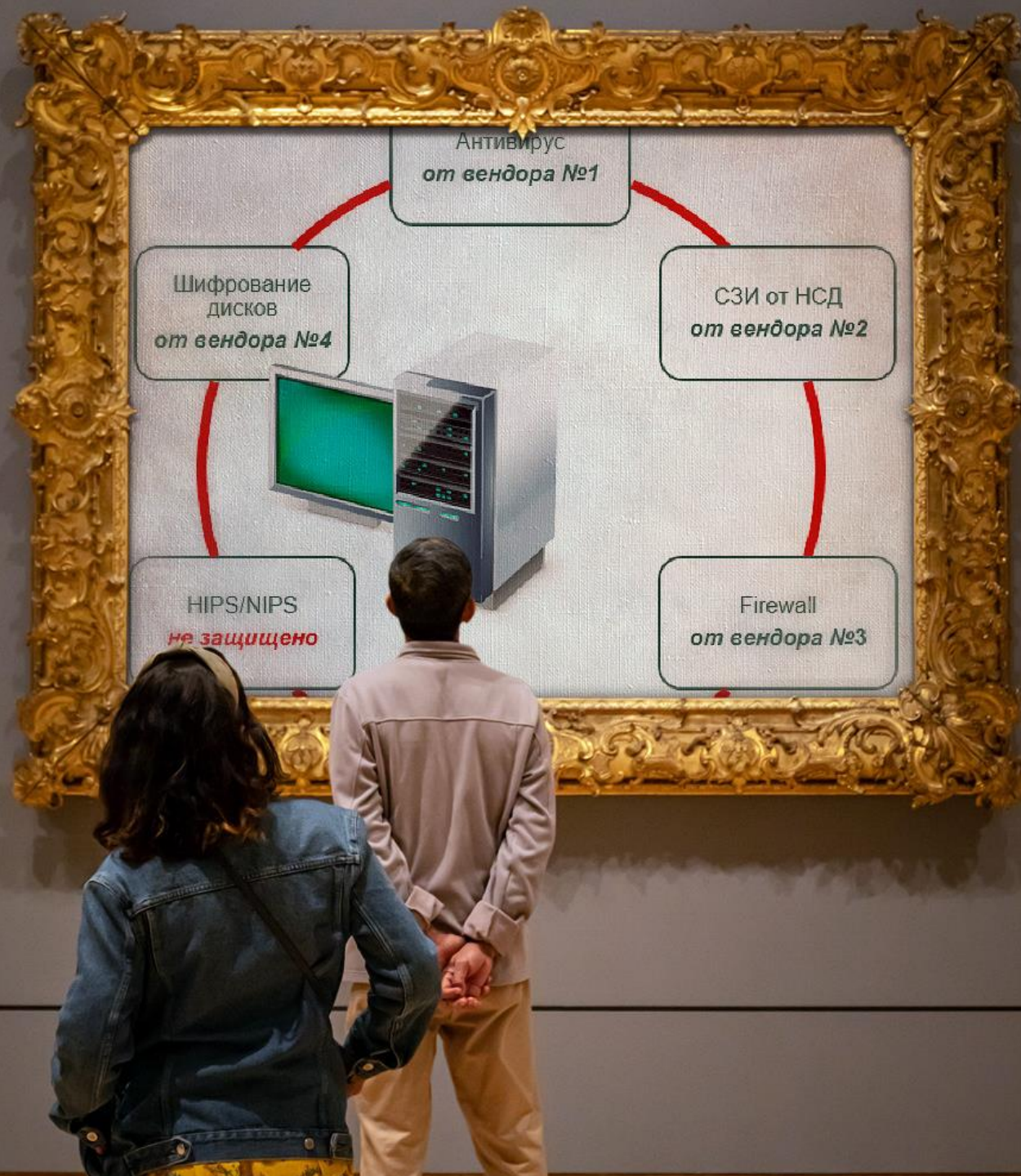
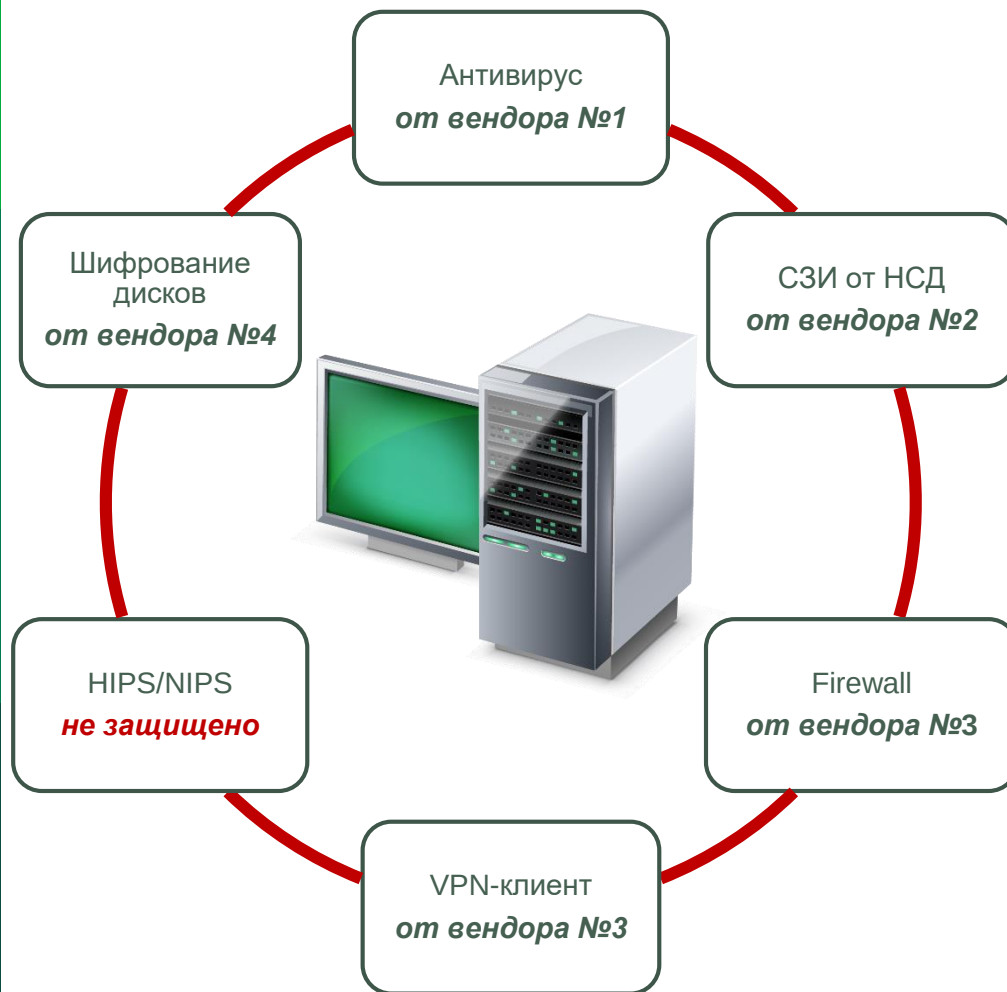
Высокая стоимость администрирования и обучения персонала работе с СЗИ

Дополнительная нагрузка на службы ИТ и ИБ по консультированию и решению проблем пользователей

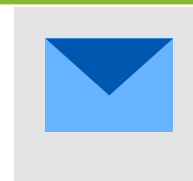
Проблемы масштабирования многовендорного решения

Высокая совокупная стоимость продуктов





|                                                                          |                                                                  |                                                                                     |
|--------------------------------------------------------------------------|------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Защита от НСД<br>к инфоресурсам компьютеров                              | Контроль подключаемых<br>к компьютеру устройств                  |  |
| Сетевая защита (межсетевой<br>экран и авторизация сетевых<br>соединений) | Централизованное<br>развертывание,<br>управление<br>и мониторинг | Защита от вирусов<br>и вредоносного ПО                                              |
| Безопасная (изолированная)<br>среда                                      | Защита дисков<br>и шифрование                                    | Доверенная<br>(программная) среда                                                   |

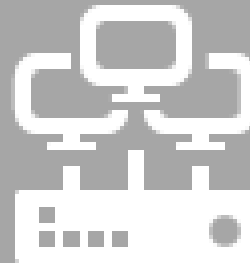


## Концепция продукта

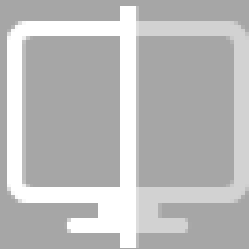
Связать воедино  
локальную защиту  
и защиту сетевой  
инфраструктуры



Централизованно  
управлять средствами  
защиты, имеющимися  
в организации



Оперативно реагировать  
на всесторонние атаки  
и события НСД



Полноценно обезопасить  
деятельность организации  
от злоумышленников —  
внешних и внутренних





КОД БЕЗОПАСНОСТИ

# КОМПЛЕКСНАЯ ЗАЩИТА НА 5 УРОВНЯХ



УРОВНИ  
ЗАЩИТЫ

ЗАЩИТНЫЕ  
МЕХАНИЗМЫ

Данные



- Теневое копирование
- Шифрование данных
- Маркировка документов

Приложения



- Регистрация и контроль запуска
- Контроль загрузки модулей и исполнения скриптов
- Контроль доступа к сети
- Контроль поведения приложений

Сеть



- Персональный межсетевой экран
- Авторизация сетевых соединений и контроль доступа к сетевым ресурсам
- VPN-клиент

Операционная  
система



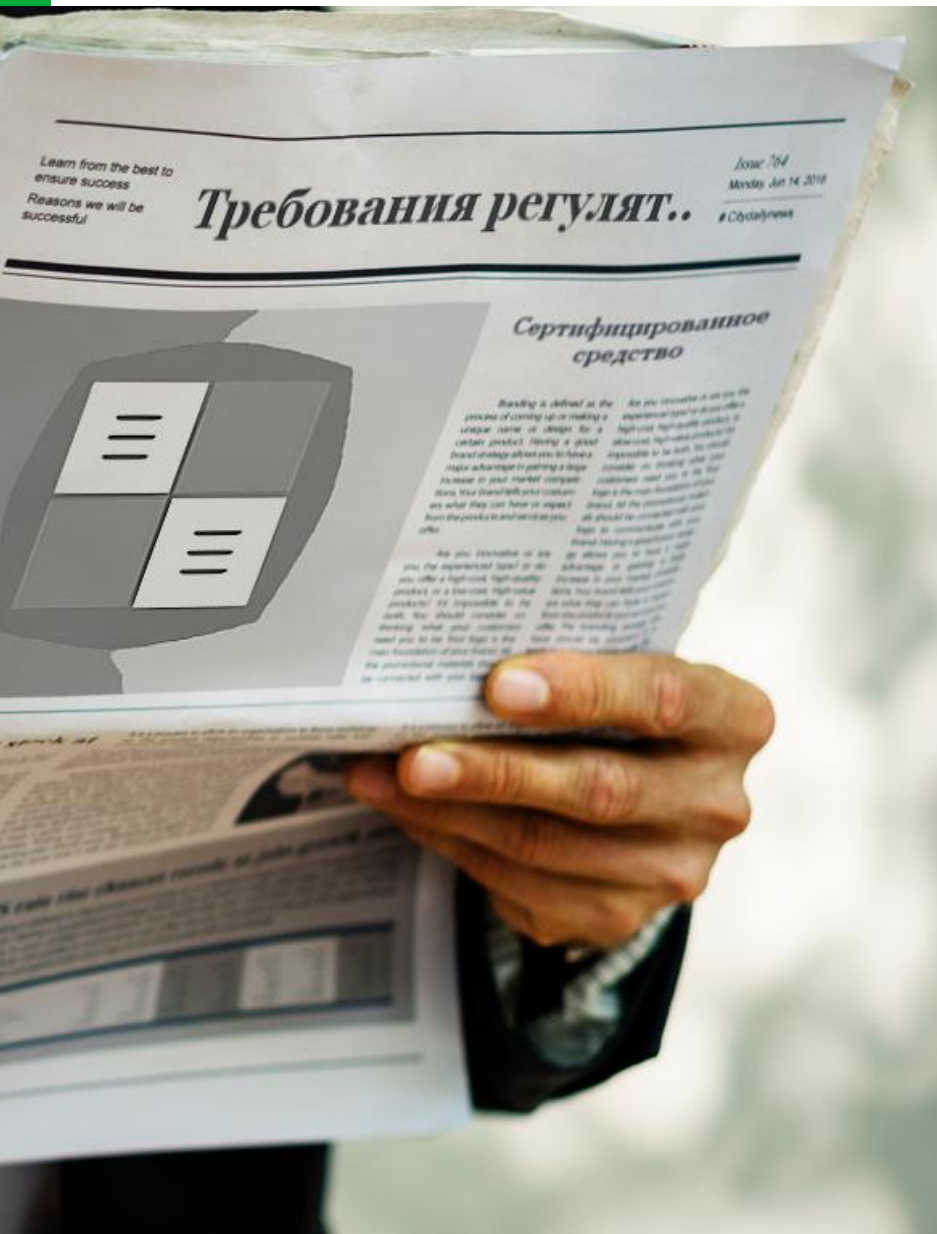
- Антивирусная защита
- Контроль входа в систему
- Управление доступом
- Контроль целостности

Периферийное  
оборудование



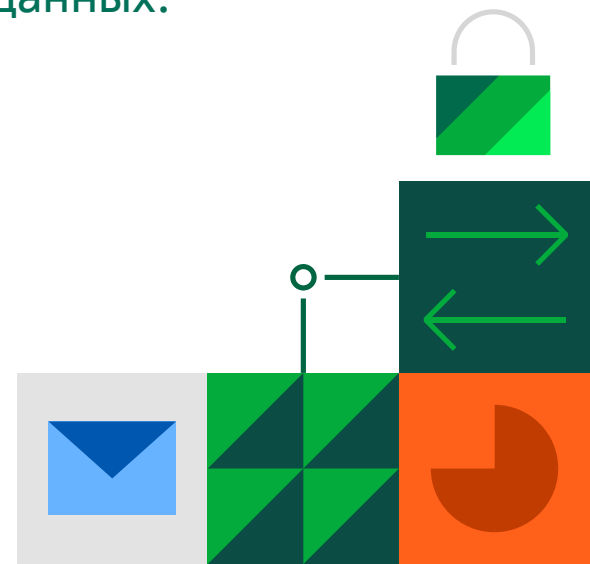
- Контроль подключения устройств и доступа к устройствам
- Интеграция со средствами доверенной загрузки (ПАК «Соболь»)

Централизованное развертывание, управление, мониторинг.  
Масштабируемость и надежность работы системы  
(иерархия серверов безопасности, репликация)



При определенных вариантах настройки система Secret Net Studio обеспечивает соответствие требованиям:

- для ГИС (приказ ФСТЭК №17);
- для ИСПДн (приказ ФСТЭК №21);
- Банка России для ИС и АС финансовых организаций (ГОСТ Р 57580.1-2017, РС БР ИББС-2.8-2015 от 01.05.2015);
- для АСУ ТП (приказ ФСТЭК №31);
- для значимых объектов КИИ (приказ ФСТЭК №239);
- по нейтрализации банками угроз безопасности, актуальных при обработке биометрических персональных данных.



## ФСТЭК России:

- по 4 уровню доверия,
- по 5 классу защищенности СВТ,
- по 4 классу защиты СКН (ИТ.СКН.П4.ПЗ),
- по 4 классу защиты САВЗ (ИТ.САВЗ.А4.ПЗ, ИТ.САВЗ.Б4.ПЗ, ИТ.САВЗ.В4.ПЗ, ИТ.САВЗ.Г4.ПЗ),
- по 4 классу защиты МЭ тип "В" (ИТ.МЭ.В4.ПЗ),
- по 4 классу защиты СОВ (ИТ.СОВ.У4.ПЗ),
- может применяться в АС до класса 1Г включительно, ИСПДн УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до класса включительно.

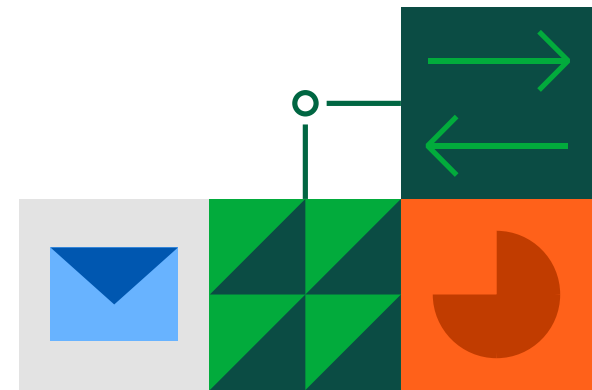


## ФСБ России:

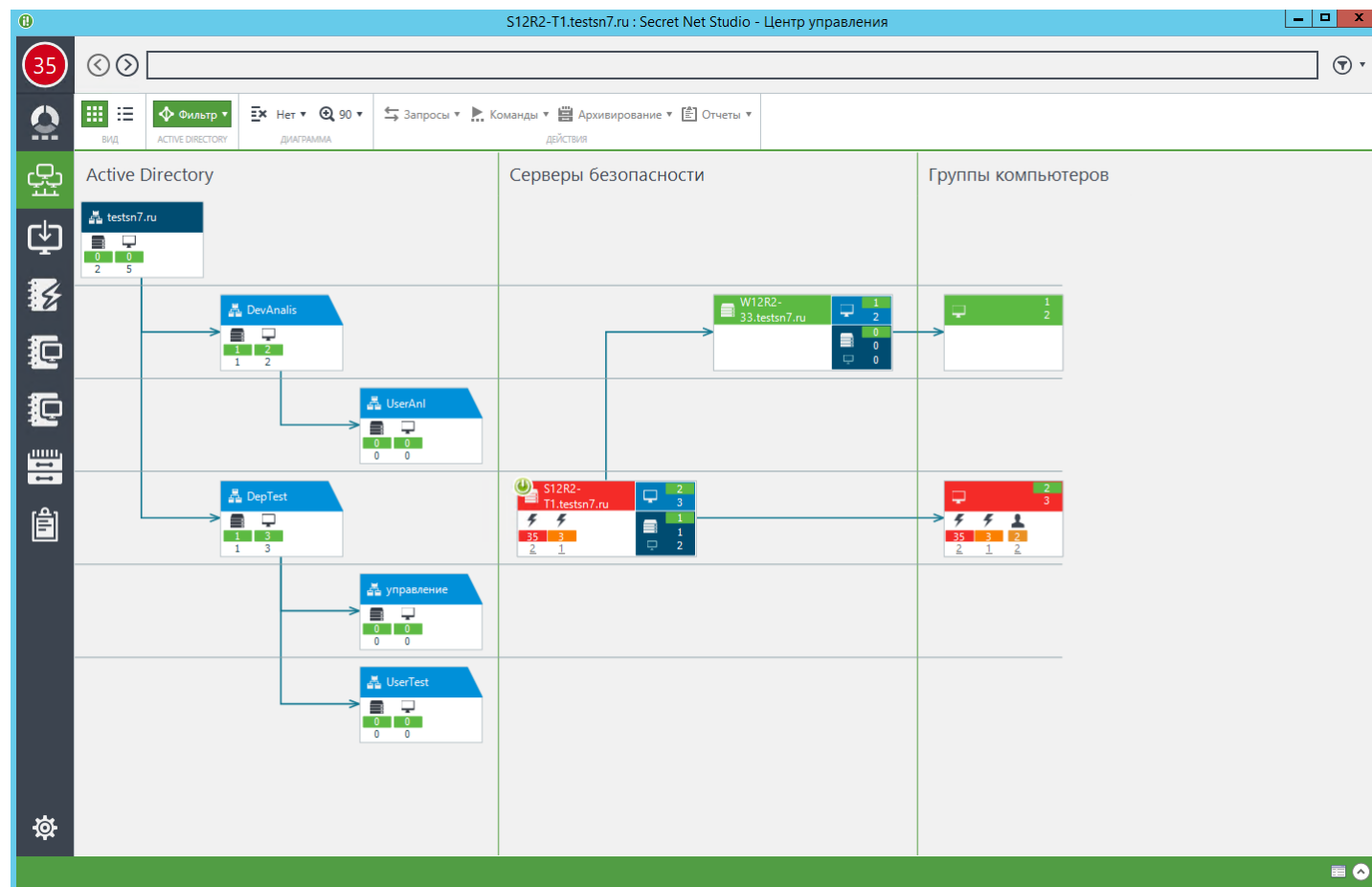
- для класса АКЗ при совместном использовании с АПМДЗ соответствующего класса.

## Минобороны России:

- дополнительная сертификация в системе сертификации СЗИ Минобороны России не требуется.



- Возможность построения иерархии серверов безопасности SNS.
- Обеспечение безопасности работы отдельных подразделений с соответствующей конфиденциальной информацией (бухгалтерия, финансовая служба, БД клиентов и т.д.).
- Защита на уровне данных (хранение информации в зашифрованных контейнерах и теневое копирование).
- Защита на уровне приложений (ЗПС).
- Защита на уровне сети (межсетевой экран и авторизация сетевых соединений).
- Защита на уровне ОС (усиленный вход в систему, антивирус, дискреционный контроль доступа, затирание информации, контроль устройств, контроль печати).







Server.sns.local : Secret Net Studio - Центр управления

Навигация

Начало

Панель инструментов

Active Directory

Серверы безопасности

Группы компьютеров

Разделы

Поле объектов, политик, настроек

Текущие события журнала сервера

Настройки подключения и отображения

настройки центра управления

| Тип                 | Дата и время                              | Событие                     | Описание |
|---------------------|-------------------------------------------|-----------------------------|----------|
| 12.01.2019 20:33:22 | Запрос конфигурации.                      | Конфигурация загружена.     |          |
| 12.01.2019 20:33:10 | Открытие сессии. Сервер Server.sns.local  | Запрос отправлен на сервер. |          |
| 12.01.2019 20:02:33 | Заккрытие сессии. Сервер Server.sns.local | Сессия закрыта.             |          |
| 12.01.2019 20:02:32 | Заккрытие сессии. Сервер Server.sns.local | Запрос отправлен на сервер. |          |
| 12.01.2019 20:00:21 | Запрос конфигурации.                      | Конфигурация загружена.     |          |
| 12.01.2019 20:00:21 | Событие об изменении конфигурации.        | Изменилась иерархия ОУ.     |          |

Подключен: Server.sns.local

Окно событий

...the importance of these answers in the graded response to the company's target. Marketing managers should manage and then reorganize the business of marketing that has to do with the company's target.

...and the other side of the road, the old quarry and the new quarry.

...with the right twist of  
...your sales and market

When you already have your marketing plan should work out. After some time it will also show you how your sales are going through networking, advertising and other sales and activities to its new customers buying cycle and increasing sales. The marketing plan should be able to show you how your sales are followed up and the results of your efforts.

[illegible]Invested in  
cases

...based on how you gain  
...customers. A market-  
...making good messages with  
...approaches in order to  
...sales and marketing

Putting your strategy into action is how your marketing plan should work. Marketing budgets will be set, at the same time it will also show you how you're going to work with your targets, it might include things like advertising etc. Having the perfect timing with your activities to fit your customers buying cycles will help you saving money and maximizing sales. The marketing plan should be comprehensive. It should have the details on how your sales are followed up and the activities your doing to develop your offers.

Lastly, improvement should be measured implicitly and summed in order for you to know what is working and what is not. This will help you

Imagine a revenue of hundred million dollars

| Resource                     | Balance Value(\$) |
|------------------------------|-------------------|
| <b>Future Benefits</b>       | <b>2,568,790</b>  |
| Worker's Compensation        | 975,810           |
| Health Insurance             | 849,870           |
| Life Insurance               | 25,000            |
| Disability Insurance         | 421,545           |
| WFO to 60-Benefit            | 276,954           |
| <b>Future Savings</b>        | <b>690,144</b>    |
| Loss of 1 month pay          | 279,910           |
| General savings              | 19,422            |
| Contribution-Healthcare      | 244,237           |
| Reserve                      | 75,380            |
| <b>Borrowing/Bank Assets</b> | <b>844,579</b>    |
| Family Income/Ret. Acct.     | 582,590           |
| Worker's individual savings  | 45,000            |
| General account              | 216,989           |
| <b>Settlement Assets</b>     | <b>461,771</b>    |
| Worker's Status              | 182,790           |
| Healthcare-Contribution      | 279,981           |
| <b>Total Resources</b>       | <b>4,567,238</b>  |

## Stock Market Strategy

Marketing strategy's goal is to increase sales and achieve advantage over other firms. It includes short-term and long-term activities of marketing that help in the analysis of a company's situation and contribute to its objectives. The strategy has within it the plan that you give sales by acquiring and keeping customers. A marketing strategy involves making good messages with the right kind of marketing approaches. It includes how you manage your sales and marketing activities. Putting your strategy into action allows you to see how your marketing plan should work. Marketing objectives will be set at the same time. You will also see how your plan should work with your targets, etc.



Putting your strategy into action is how your marketing plan should work. Marketing budgets and be set at the same time it will also show you how you're going to work with your targets, it maybe through networking, advertising etc. Having the perfect timing with your customers to fit your customers buying cycles will help you increase money and maximising sales. The marketing plan

should be innovative. It should have the ability to track your sales, are followed up and the collection your doing to develop your offers.

It is a process to allow an organization to focus resources on the greatest opportunities to increase sales and achieve the company's target. Marketing strategy goal is to increase sales and achieve advantage over other competitors.



As the owners of a brand, you are responsible for making a product name, or design, for a certain product stand out in a crowded market. A good brand strategy can help you to have a higher probability of a large increase in the market penetration of your brand, both now and later. Here are what they can do for you: from the product and services you offer.

# THE DAILY

Learn from the best in  
small business  
because we will be  
successful.

© 2004 Blackwell Publishing Ltd

# SECRET NET STUDIO

## Сценарии применения

#### US RATE RISE CHANCES REDECE AS 1985 GROWTH SLOWS

11.2 Process to allow an organization to be measured on the greatest opportunity to improve sales and achieve the company's larger marketing strategy is a goal to increase sales and achieve the company's other responsibilities. It involves defining and measuring key activities in relation to the firm's goals, the principles of a company's strategy and objectives, and the marketing objectives will be based on the firm's goals, the marketing and sales objectives.

During your interview, it's smart to show your employer that you should work. Management might be able to tell if you're this kind of person. But how can you prove you're going to work and grow here? Probably by showing how you're planning to do it. Showing the perfect timeline when your activities in 18 years coincide with the company's goals will help you leave no room for misunderstanding. This planning you should do immediately. It should have a week or two from your home or office and be available for you during the interview. After all, it's a promise to show an employer to focus resources on the people responsible to maintain focus and achieve the company's target. Managing strategy, not a company's goals and policies, is the most important competitive



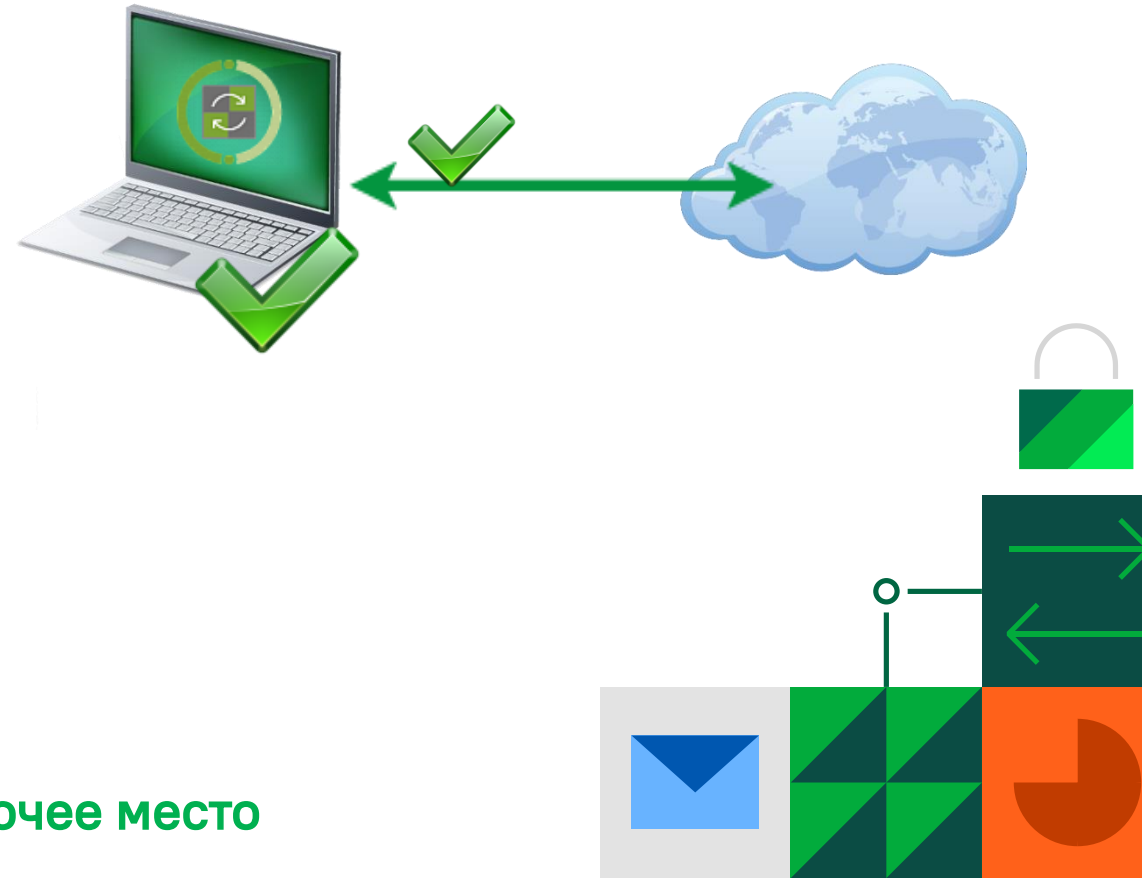
What does success mean in the global marketplace? It means being able to deliver a product or service that meets the needs of your target market. It means being able to compete effectively in a global market. It means being able to deliver a product or service that meets the needs of your target market. It means being able to compete effectively in a global market.

[illegible]

THE WORLD DISMISSED UP

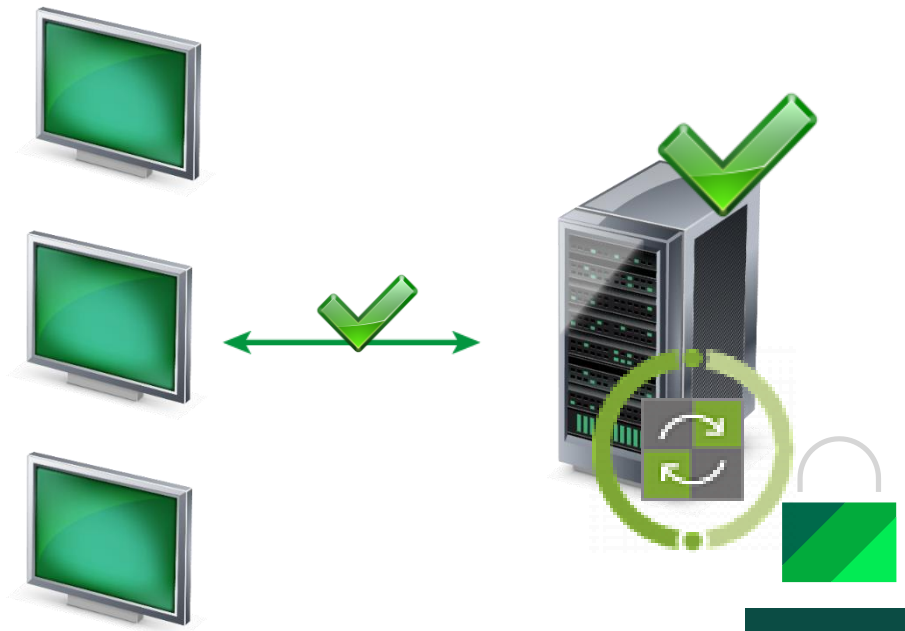


- Компьютер надежно защищен от внешних вторжений и вредоносного ПО, информация защищена на случай кражи оборудования.
- Защита на уровне данных (хранение информации в зашифрованных контейнерах).
- Защита на уровне приложений (замкнутая программная среда).
- Защита на уровне сети (контроль трафика и защита передачи конфиденциальной информации, обнаружение и предотвращение вторжений).
- Защита на уровне ОС (антивирус, затирание данных).

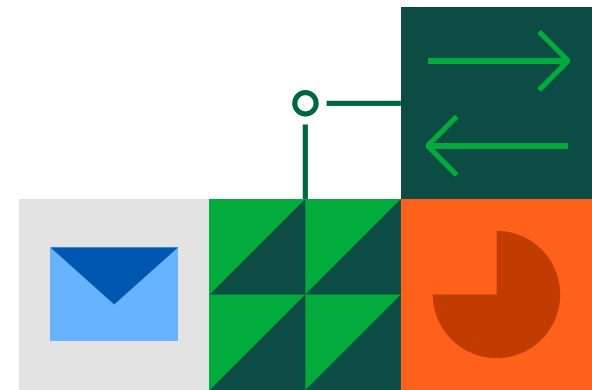


Обособленное рабочее место

- Надежное разграничение доступа к терминальному серверу с разделением для пользователей правил сетевого доступа к конфиденциальной и неконфиденциальной информации.
- Защита на уровне данных (теневое копирование, отслеживание действий отдельного пользователя).
- Защита на уровне сети (межсетевой экран, авторизация сетевых соединений, обнаружение и предотвращение вторжений от недоверенных компьютеров и внешних источников).
- Защита на уровне ОС (усиленный вход в систему, антивирус, контроль устройств, изоляция модулей — запрет взаимодействия между процессами разных пользователей).



Защита терминального сервера



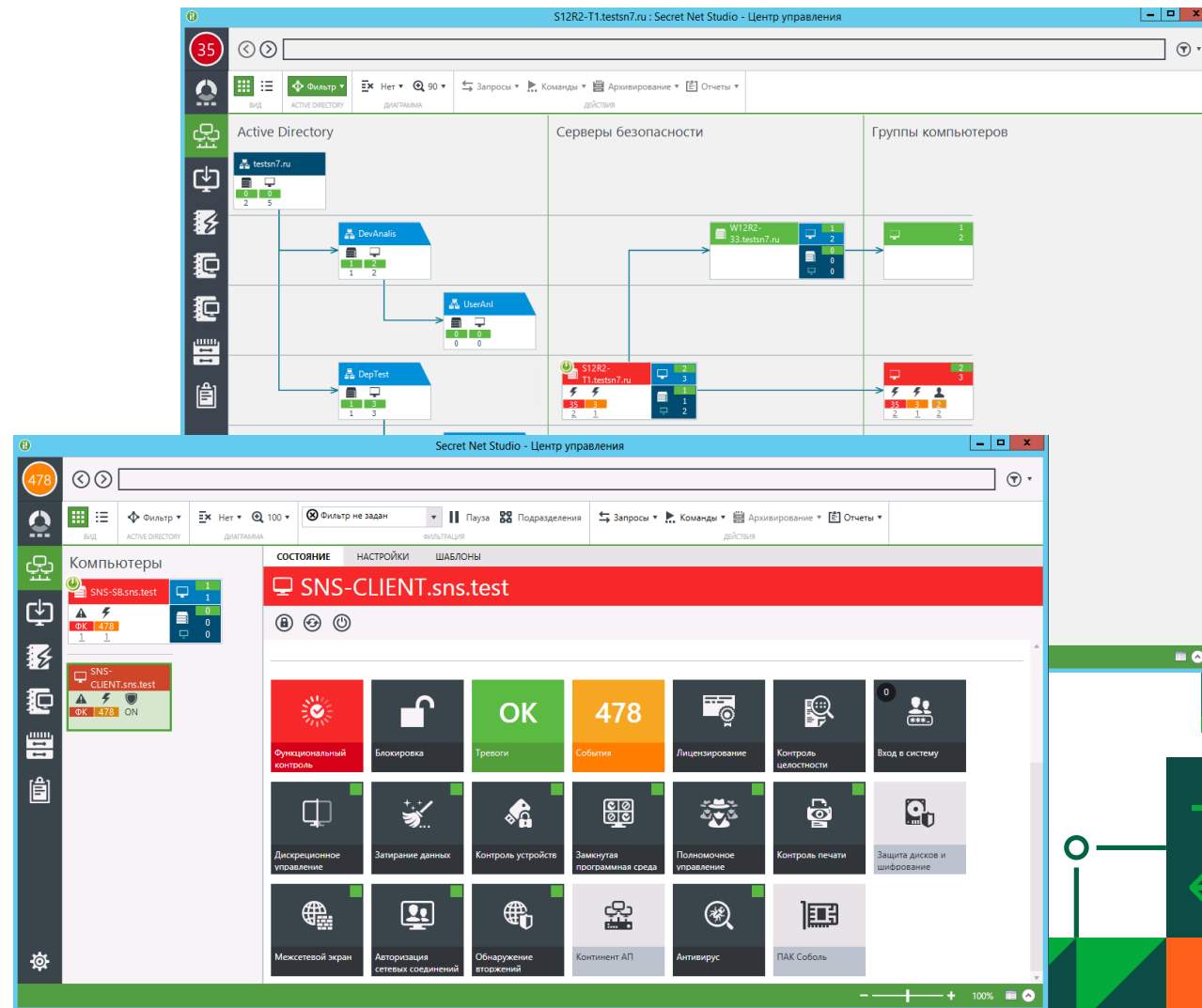


Централизованное  
управление

6,25

6,00

- Политики для управления настройками защитных компонентов, поддержка иерархии.
- «Плиточный» интерфейс для обзора модулей защиты.
- Два типа оперативных команд: общие (блокировка станции, применение политик, выключение и т.д.) и специализированные (по модулям защиты).
- Управление основными настройками из панели статуса.
- Быстрый переход к политикам и полным настройкам.



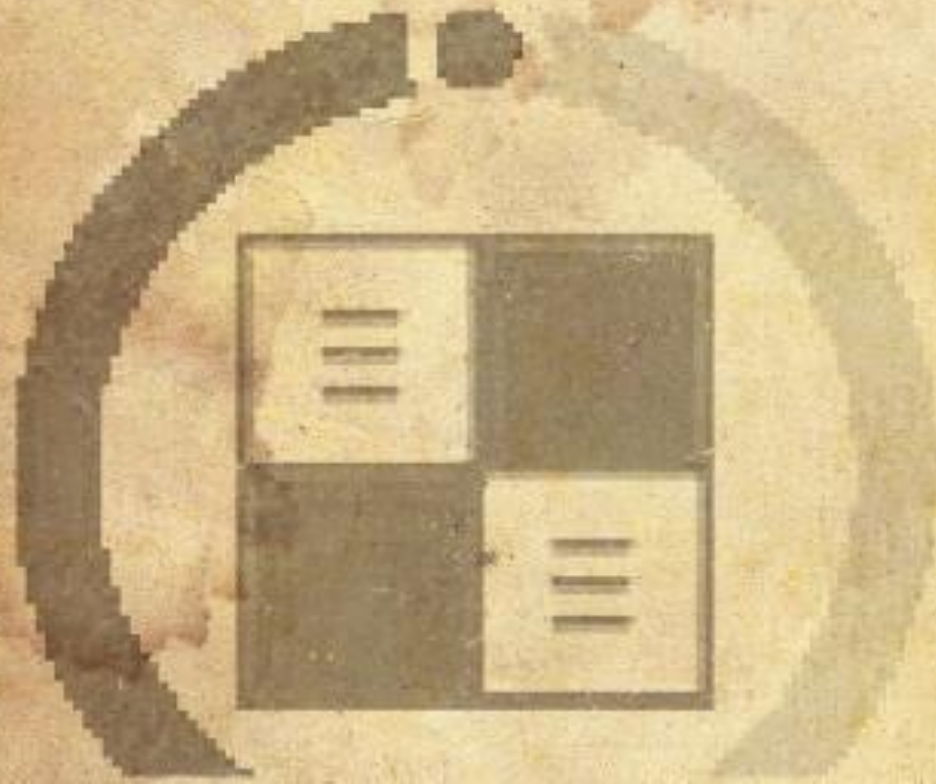


КОД БЕЗОПАСНОСТ

ПРИВИЛЕГИИ

# SECRET NET STUDIO

## Повышение полномочий





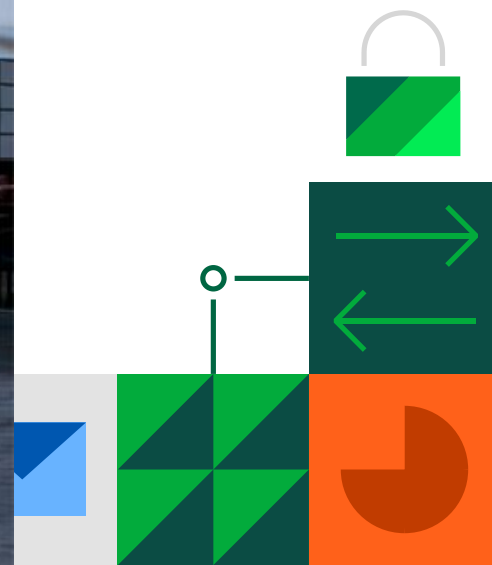
Привилегии для работы с программой управления

Управление привилегиями пользователей для работы с программой управления осуществляется в группе "Привилегии пользователей". Группа присутствует при выборе сервера безопасности.

Пользователям и группам пользователей могут быть назначены следующие привилегии:

- **"Просмотр информации"** — привилегия для подключения к серверу безопасности и просмотра информации, построения отчетов, просмотра списка карантина антивируса;
- **"Редактирование иерархии и параметров объектов"** — привилегия для редактирования конфигурации объектов и управления параметрами в разделе "Параметры";
- **"Выполнение оперативных команд"** — привилегия на выполнение команд оперативного управления;
- **"Редактирование политик"** — привилегия для управления параметрами в разделах "Политики" и "Регистрация событий";
- **"Квитирование сообщений о тревогах"** — привилегия на выполнение команд квитирования событий тревоги;
- **"Сбор журналов по команде"** — привилегия на выполнение внеочередной передачи локальных журналов компьютеров;
- **"Архивирование/восстановление журналов"** — привилегия на выполнение процедур архивирования или восстановления централизованных журналов;
- **"Загрузка СПС из файла"** — привилегия на выполнение команды загрузки в базу сервера безопасности собранных сведений о состоянии программной среды компьютера;
- **"Утверждение паспорта ПО"** — привилегия на выполнение команды утверждения проекта паспорта в качестве текущего паспорта компьютера;
- **"Синхронизация базы данных паспортов ПО"** — привилегия на выполнение команды синхронизации сведений о паспортах, расположенных на сервере безопасности;
- **"Удаление паспорта ПО"** — привилегия на выполнение команды удаления паспортов, кроме текущего утвержденного паспорта;
- **"Редактирование политик самозащиты"** — привилегия для управления параметрами механизма самозащиты.

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.



- Общий мониторинг защищенности системы.
- Разбиение защищаемых компьютеров на группы для наблюдения и отдельного отображения состояний.
- Оперативная передача событий НСД и других важных событий на панель мониторинга, по e-mail или локальным оповещением.
- Тревоги — отдельный тип событий высокой степени важности.
- Возможность квитирования событий — проставления отметок о прочтении и добавления комментариев к событиям.

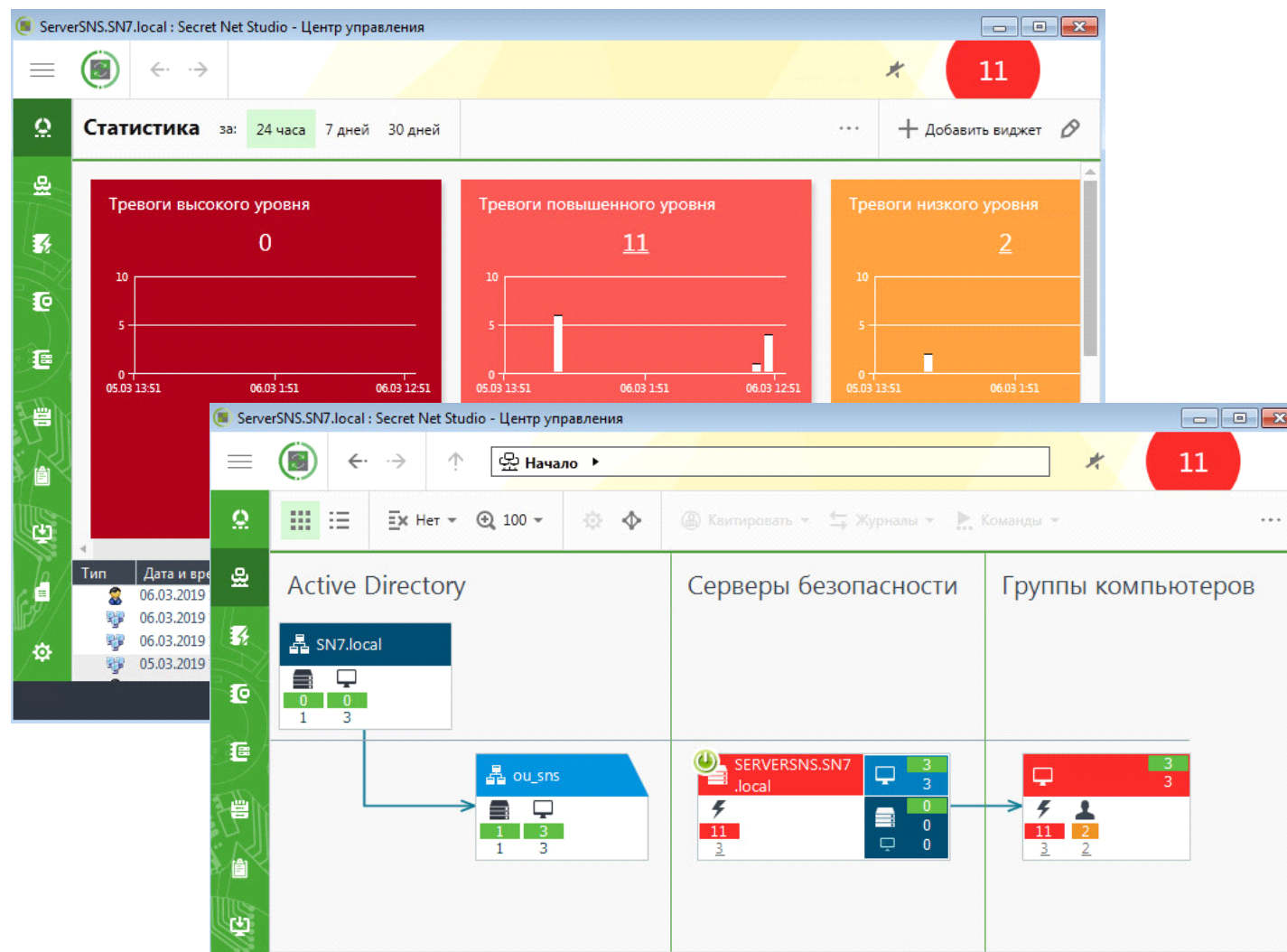




Табл.6 Поток событий и средний размер записей на сервере безопасности

| Журналы                  | Среднее количество событий в секунду (EPS) | Средний размер записи (байт) |
|--------------------------|--------------------------------------------|------------------------------|
| Штатные журналы ОС       | 3                                          | 1000                         |
| Журнал Secret Net Studio | 0,05                                       | 800                          |

Табл.7 Поток событий и средний размер записей на клиенте

| Журналы                  | Среднее количество событий в секунду (EPS) | Средний размер записи (байт) |
|--------------------------|--------------------------------------------|------------------------------|
| Штатные журналы ОС       | 1                                          | 1000                         |
| Журнал Secret Net Studio | 0,05                                       | 800                          |

Табл.8 Объем журналов

| Журналы                                          | Количество событий в день | Заполнение БД за день (МБ) <sup>1</sup> | Объем журналов в БД за 7 дней (МБ) <sup>2</sup> | Объем журналов в архиве за 1 год (МБ) <sup>3</sup> |
|--------------------------------------------------|---------------------------|-----------------------------------------|-------------------------------------------------|----------------------------------------------------|
| <b>Сервер безопасности, 1 компьютер</b>          |                           |                                         |                                                 |                                                    |
| Штатные журналы ОС                               | 259 200                   | 259,2                                   | 1 814,4                                         | 2 365                                              |
| Журнал Secret Net Studio                         | 4 320                     | 3,5                                     | 24,2                                            | 31,5                                               |
| <b>Клиент Secret Net Studio, 100 компьютеров</b> |                           |                                         |                                                 |                                                    |
| Штатные журналы ОС                               | 8 640 000                 | 8 640                                   | 60 480                                          | 78 840                                             |
| Журнал Secret Net Studio                         | 432 000                   | 345,6                                   | 2 419,2                                         | 3 153                                              |
| <b>Всего для сервера безопасности и клиентов</b> |                           |                                         |                                                 |                                                    |
|                                                  |                           | <b>9 248,3</b>                          | <b>64 737,8</b>                                 | <b>84 390</b>                                      |

## Единый агент безопасности

- Отсутствие конфликтов между различными защитными подсистемами.
- Снижение общей нагрузки на защищаемый компьютер за счет отсутствия дублирования функций.

## Снижение сложности защищаемой системы

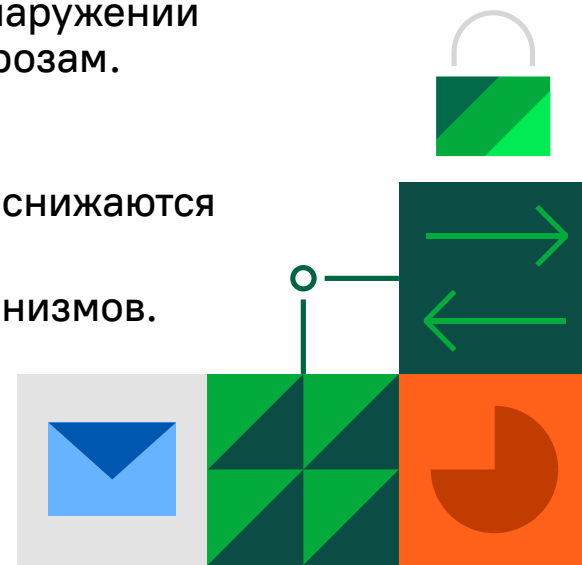
- Сокращение «зоопарка» и простота обеспечения согласованной работы различных защитных подсистем.
- Возможность создания единой политики безопасности для всей организации или отдельных политик безопасности по отделам, уровням обрабатываемой информации или филиалам, с автоматическим применением политики для всех защищаемых компьютеров.

## Скорость реакции на угрозы

- Возможность оперативно изменить глобальную политику из одной точки, чтобы при обнаружении инцидентов информационной безопасности мгновенно противостоять возникающим угрозам.

## Экономическая составляющая

- Единая архитектура и единая консоль облегчают освоение новых защитных подсистем, снижаются затраты на обучение персонала и количество задействованных сотрудников.
- Покомпонентное лицензирование, возможность покупки только нужных защитных механизмов.
- Возможность расширения лицензии и дозакупки компонентов.
- Объемные скидки по количеству лицензий и количеству компонентов в них.





КО

# Требования для компонентов SNS

1Я



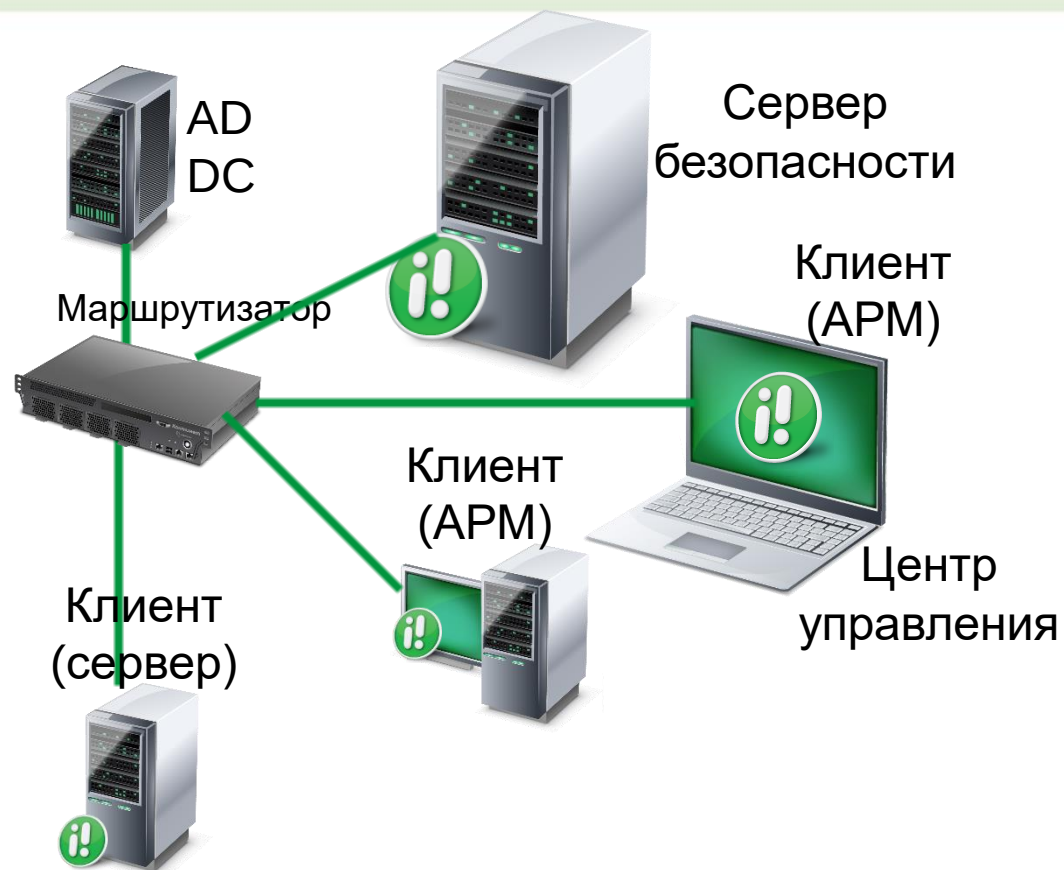
Поддержка  
Windows 10;  
Windows 8.1 Rollup Update KB2919355  
Windows 7 SP1;  
Windows Server 2012/Server 2012 R2 R  
Windows Server 2008 R2 SP1;  
Windows Server 32- и 64-разрядные вери  
Поддерживаются 32- и 64-разрядные вери  
устанавливаемыми пакетами обновлений и  
Windows Server 2012/Server 2012 R2 R  
Windows Server 2008 R2 SP1  
Windows Server 2012/Server 2014 (



| № | Приложение                 | Поддерживаемые ОС                                                                                                                                                                                                                                                                                                                                                                   |
|---|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Клиент<br>Центр управления | <ul style="list-style-type: none"><li>• Windows 10;</li><li>• Windows 8.1 Rollup Update KB2919355;</li><li>• Windows 7 SP1;</li><li>• Windows Server 2016;</li><li>• Windows Server 2012/Server 2012 R2 Rollup Update KB2919355;</li><li>• Windows Server 2008 R2 SP1;</li></ul> Поддерживаются 32- и 64-разрядные версии ОС с установленными пакетами обновлений не ниже указанных |
| 2 | Сервер<br>Безопасности     | <ul style="list-style-type: none"><li>• Windows Server 2016;</li><li>• Windows Server 2012/Server 2012 R2 Rollup Update KB2919355;</li><li>• Windows Server 2008 R2 SP1</li></ul>                                                                                                                                                                                                   |
| 3 | СУБД                       | СУБД MS SQL 2008 R2 SP1/2012 SP1/2014 (включая Express-редакции)                                                                                                                                                                                                                                                                                                                    |



# ПРОГРАММНЫЕ ПАКЕТЫ (СЕТЕВОЙ РЕЖИМ)



SECRET NET STUDIO  
КОД БЕЗОПАСНОСТИ

Средства локального управления

- Клиент SNS
- СБ SNS

Средства централизованного управления

- ЦУ SNS
- Сервер безопасности

- Драйвер Secret Net Card
- Дополнительное ПО
- Документация
- Обзор диска

КОД БЕЗОПАСНОСТИ



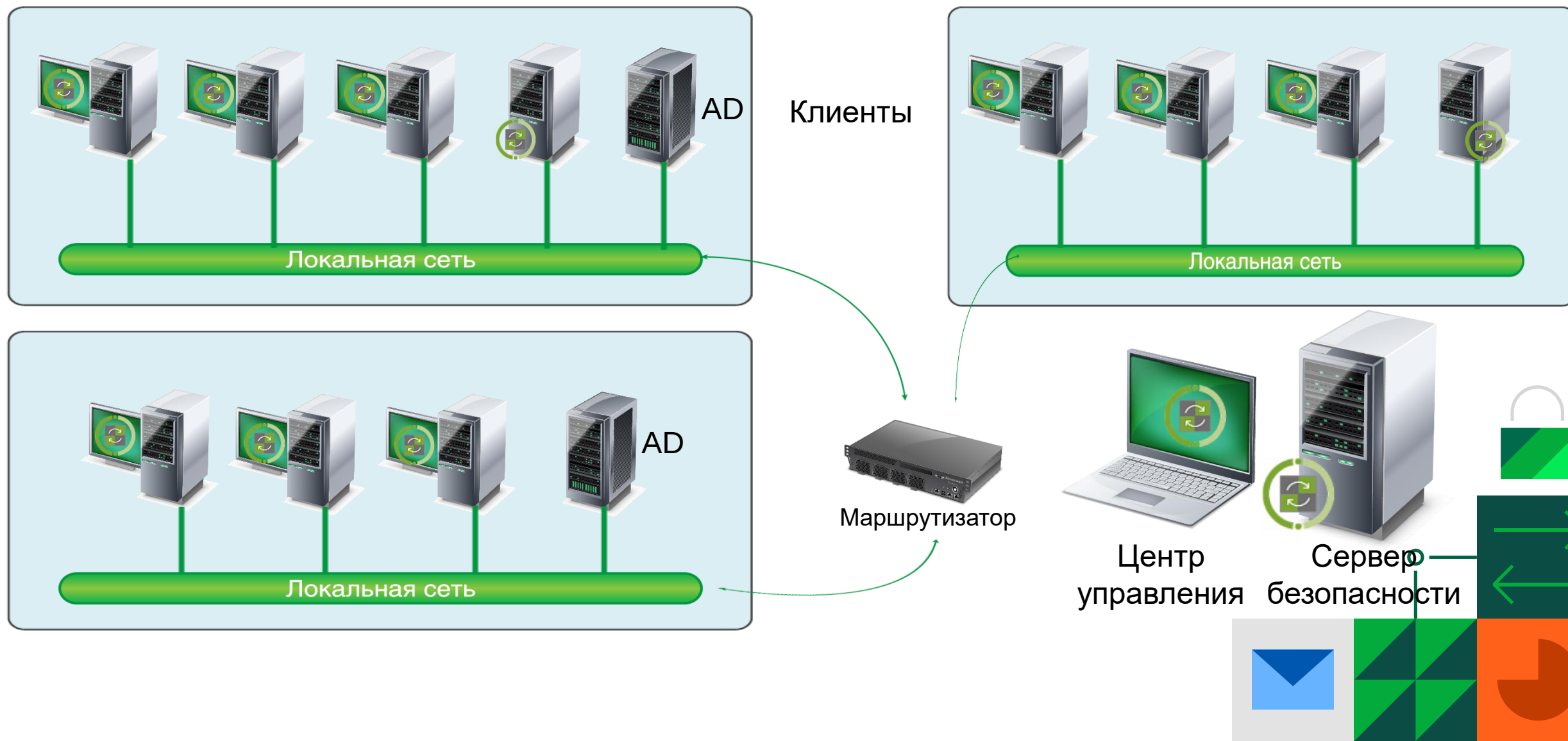
# СХЕМА лицензирования



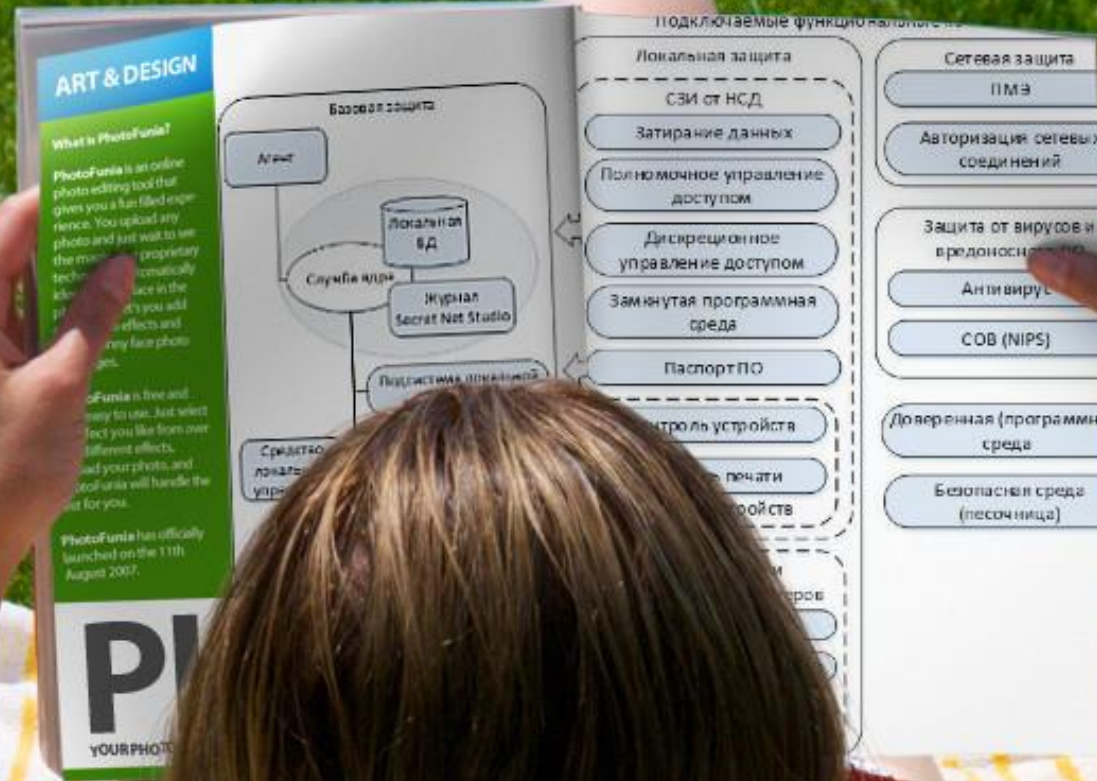
- Защита от НСД (затирание данных, Паспорт ПО, полномочное управление доступом, дискреционное управление доступом, ЗПС).
- Контроль устройств (контроль устройств, контроль печати).
- Защита дисков и шифрование.
- Персональный межсетевой экран (ПМЭ, авторизация сетевых соединений).
- Антивирус.
- Средство обнаружения вторжений (NIPS).
- Безопасная (изолированная) среда.
- Доверенная среда.

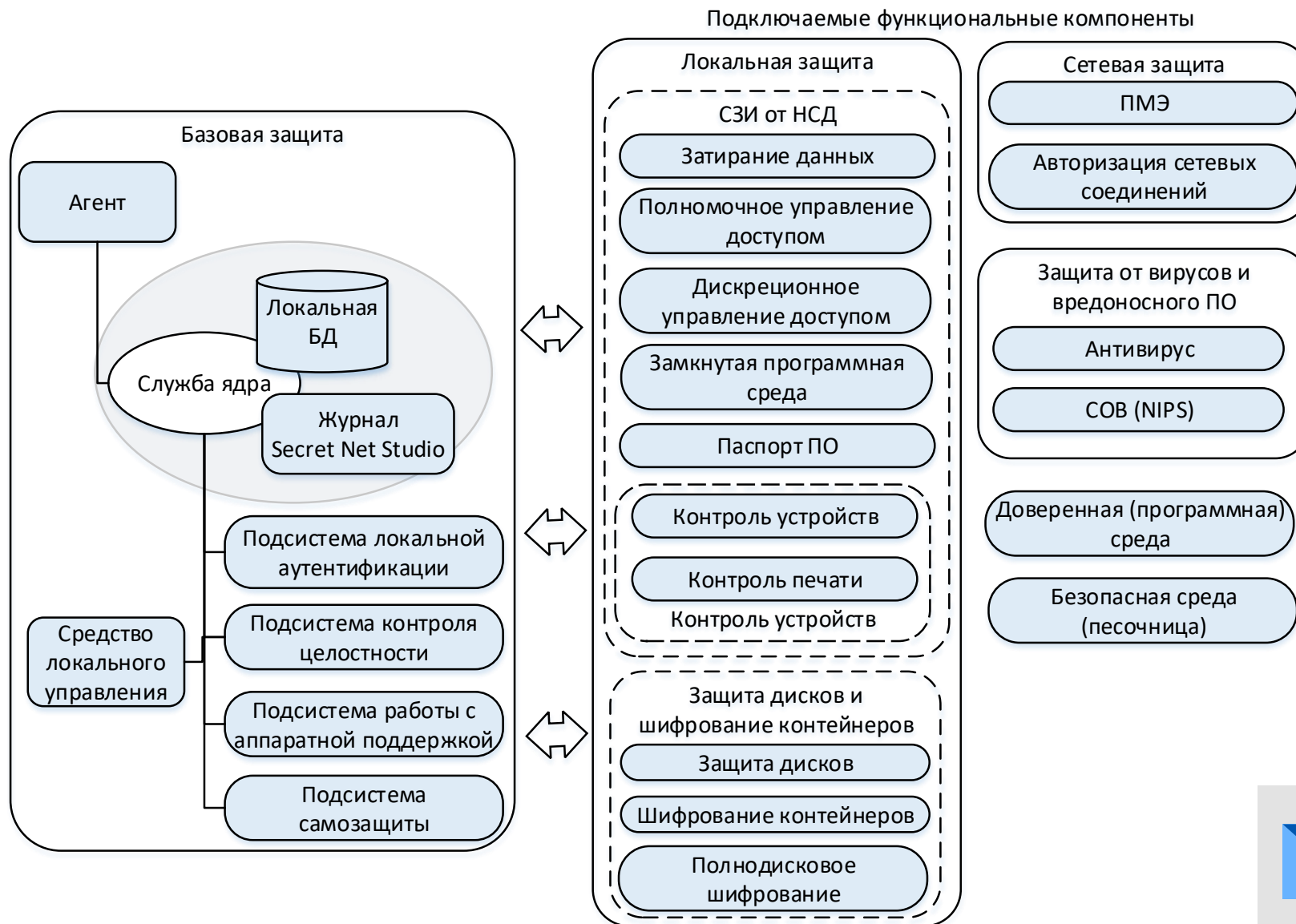


\*Срочные лицензии – стандартно на 1 год, технически допустим любой срок



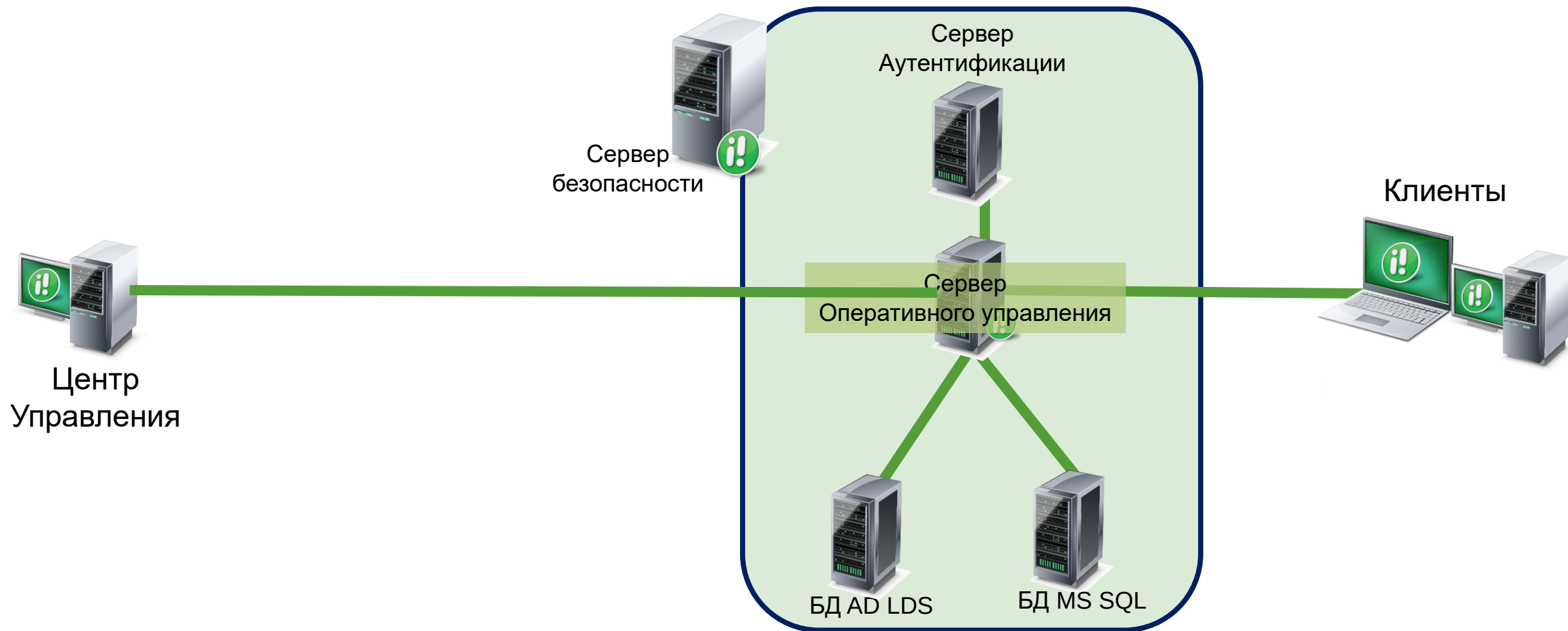
# Структурная схема клиента







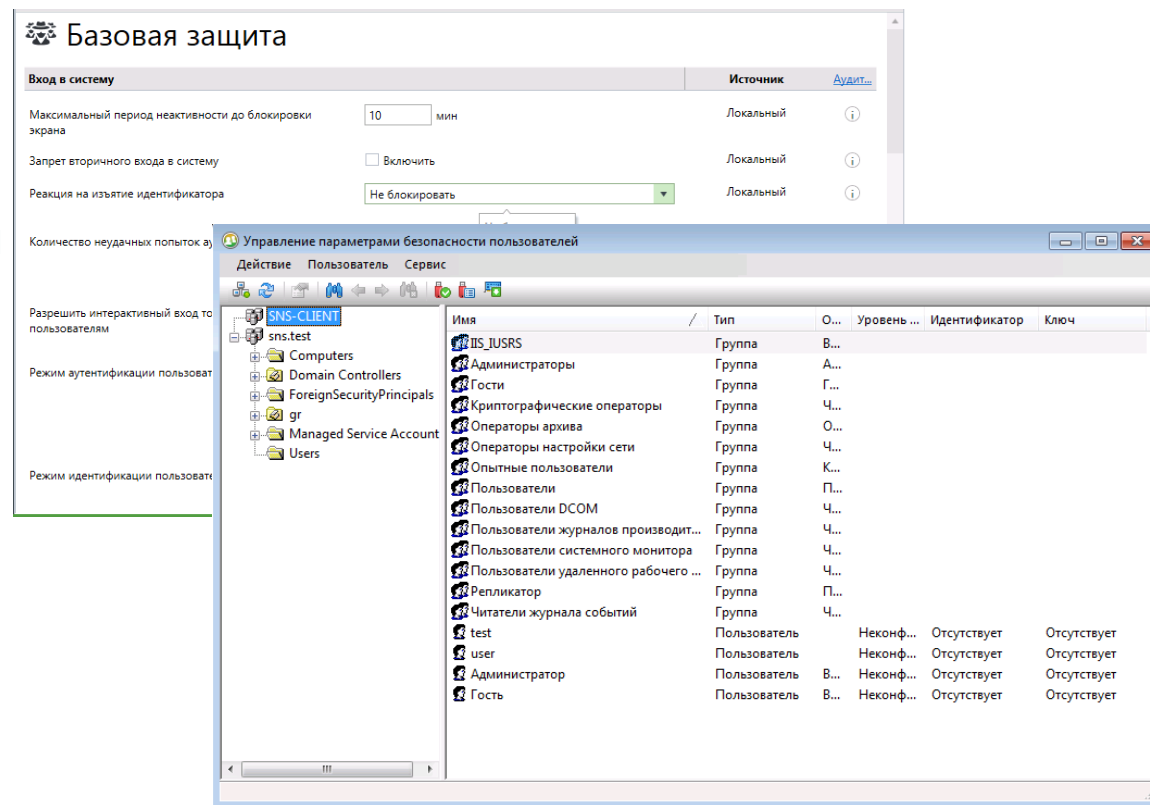
# Структура Сервера Безопасности (СБ)





## Усиленный вход в систему

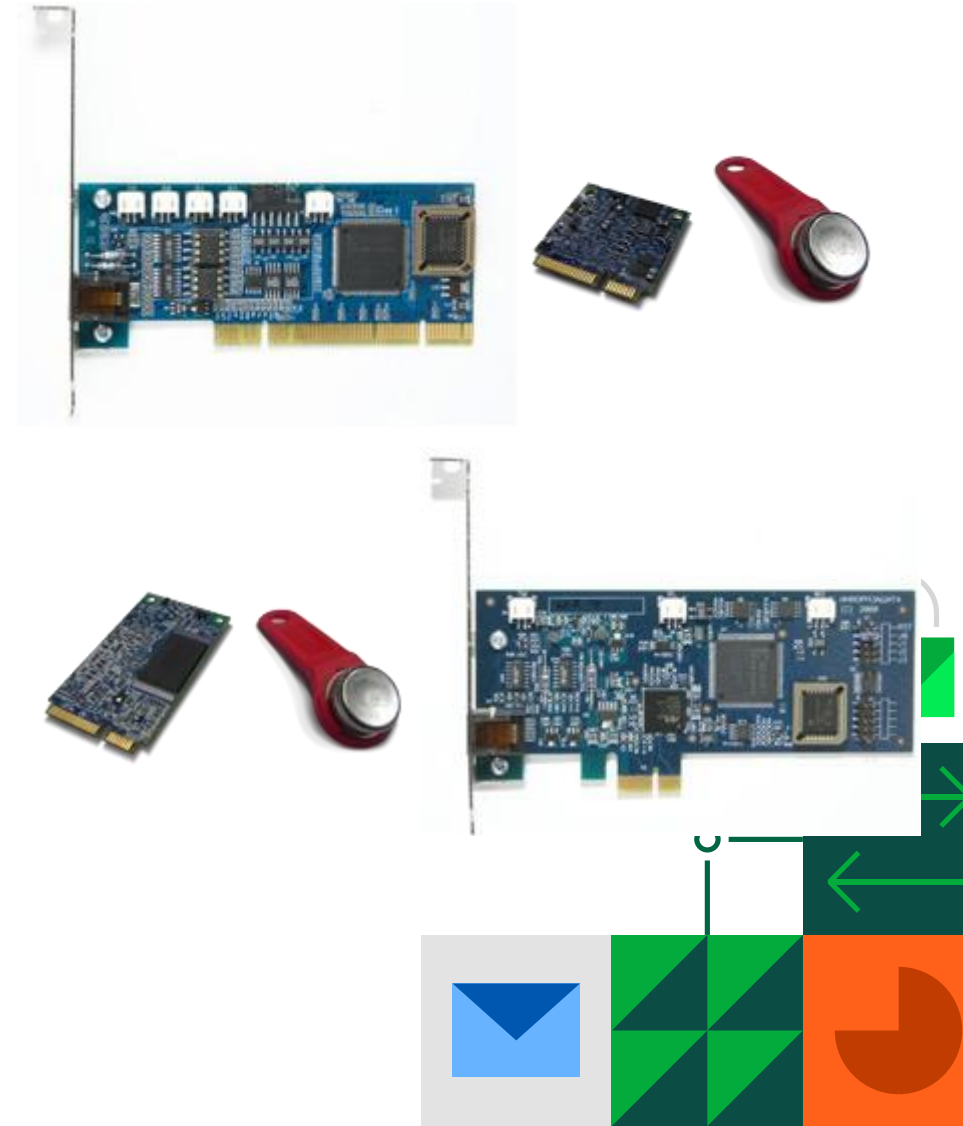
- Поддержка двухфакторной аутентификации и электронных идентификаторов eToken, Rutoken, ESMART, JaCarta, Guardant ID, vdToken, R301 Foros и iButton.
- Собственная усиленная парольная аутентификация и парольные политики.
- Политики блокировки сеанса при неактивности или изъятии идентификатора.
- Работа с локальными и доменными пользователями, поддержка терминальных серверов и VDI.
- Гибкие настройки ограничения доступа – запрет вторичного входа (RunAs), запрет входа локальными пользователями и т.д.
- Собственная программа управления пользователями.





## Интеграция с ПАК «Соболь»

- Возможность сквозной аутентификации и управления входом в ПАК «Соболь» из Secret Net Studio.
- Возможность настройки заданий на контроль целостности для ПАК «Соболь» из интерфейса Secret Net Studio.
- Получение журналов из ПАК «Соболь».
- Работа с идентификаторами iButton (поддерживаемые типы DS1992 – DS1996), подключенными к ПАК «Соболь».





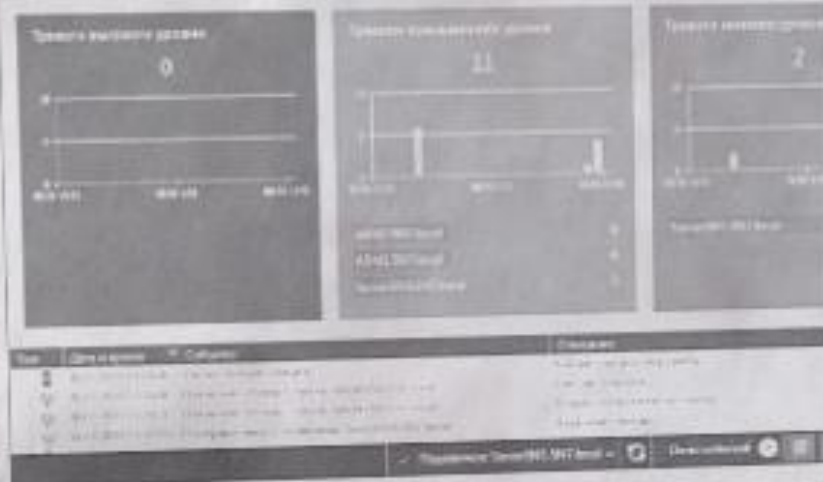
КОД

## Журналирование

Copyright © 2007 John Wiley & Sons, Ltd.



Судящаяся — Иванова Мария Ивановна



Letzte Woche hat zum Kiez Song  
hatten, beiden interessiert sich nach  
Menschen Strafe der off the Bild. Der  
vollständige Teil Song Lieder hatten.  
Horn a (Wap-hup...) Er brach mich  
wie Schokolade.

[illegible]

Source: author's calculations based on data from the Survey of Consumer Expenditures.

Das Gamsberg zeigt ungefähr so viele  
et menschlich. 1884 kann nicht wegen, 1884  
hat den Song geküßt. Alles Vordere, die  
vielleicht stammte, vielleicht nicht, in  
Wahrheit geht es natürlich um etwas an-  
deren. Es geht um Geld. Auf Gamsberg  
leben nicht alle im vorgerückten Leben.

[illegible]

Weiland, der Fotograf, und ich, dem ich Gedichte, die Lieder, die Kapitel und auch die „Mysterien“ meines Lebens“ eine unregelmäßige Projektionsfläche für Meditation und Gedankenspiele ist. Was immer ich hier lese und schreiben oder auch nur in der Hand halten, kommt an Millionen Menschen heran, und das ist ein großer Anreiz.

I sing: Wippen, so, so, so, so  
Wippen, so, so, so, so, Kinder in die  
Zukunft zu schicken, um diese Clips in ihre  
Hände, und ich will in Wahrheit einen Ge-  
fassen. Und darum was ich mit jetzt noch  
nicht, das schreie eine lange Zeit aus-  
gerufen für meine Kinder und ihre  
Kinder.

And when they reach France, Arruf and his minder (Belgian) Tattler, Maria, tell her that in their headquarters with journalists, she had Interview Summer school.

Ich bin immer noch überzeugt davon, dass die Wirtschaftspolitik, die wir heute verfolgen, die richtige ist. Ich bin auch noch der Meinung, dass die Bundesregierung die richtigen Entscheidungen getroffen hat. Ich bin auch noch der Meinung, dass die Bundesregierung die richtigen Entscheidungen getroffen hat.

[illegible]

...nachdem ich  
...und habe, so  
...den Wert  
...haben, so

...der ...  
...der ...  
...der ...

Die zwei ersten Schritte, die Sie für die tolle Deutschschule durchführen, sind das Ausfüllen des Fragebogens und das Einreichen der Karte. Die Karte enthält die Adresse, an die Sie den Fragebogen senden müssen, wenn Sie sich an der Deutschschule anmelden möchten. Bitte füllen Sie den Fragebogen so vollständig wie möglich aus, damit wir Sie besser kennenlernen können. Ihre Karte wird nicht an andere weitergegeben, sondern nur für die Deutschschule verwendet.



422 张其成讲读

[illegible]

...der Fall...

**G**leichzeitig ist das ein ständiges, hartes Rennen um die 2007er Weltmeisterschaften in Deutschland. Und das ist ein Rennen, das nicht nur die Athleten, sondern auch die Zuschauer mit Spannung erfüllt. Denn es geht um die Ehre der Nationen und um die Frage, wer der Beste ist. Und das ist ein Rennen, das nicht nur die Athleten, sondern auch die Zuschauer mit Spannung erfüllt. Denn es geht um die Ehre der Nationen und um die Frage, wer der Beste ist.

„Ich bin immer mehr zu Hause in der Natur und ich bin mehr als je zuvor Teil der Gruppe“, sagt Michael. „Die Gruppe ist das Wichtigste. Ich bin Teil der Gruppe und ich bin Teil der Gruppe.“

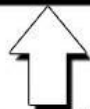
[illegible]

The wordless duet, full of wistfulness, might be seen, says the critic, as a metaphor for the relationship between the two singers. Older in years than the younger, she is a more direct singer, less much like her younger brother, who, with Adams, was much more reserved than most Westons, she felt.

[illegible]



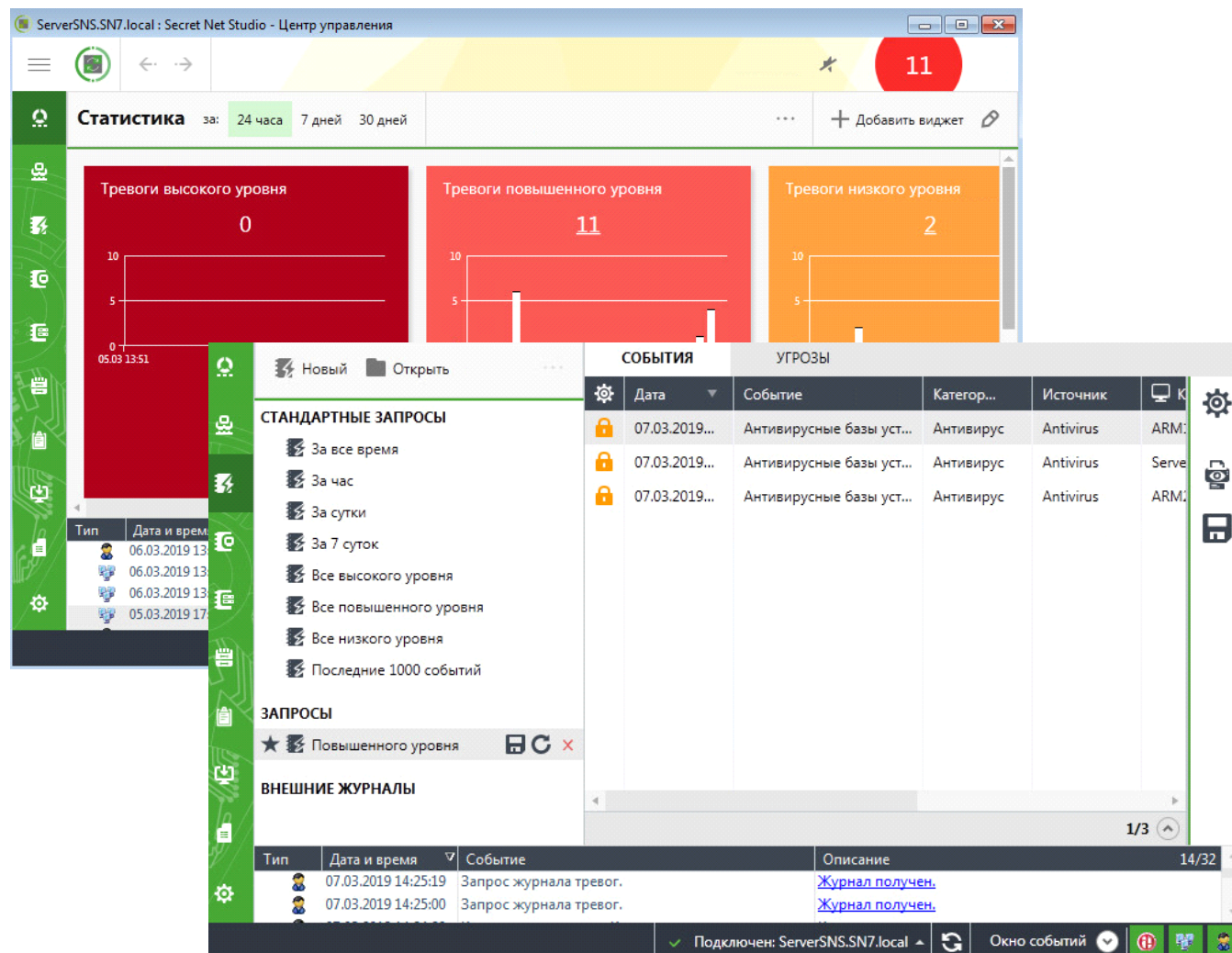
| Название сбора данных                                                                            | Источник данных | Формат  | Локальная копия        |
|--------------------------------------------------------------------------------------------------|-----------------|---------|------------------------|
|  ЖУРНАЛЫ ТРЕВОГ  | СТАНЦИИ         | *.snua  | SQL DB                 |
|  ЖУРНАЛЫ СТАНЦИЙ | СТАНЦИИ         | *.snlog | \OmsAgentEvtCopy\*.evt |
|  ЖУРНАЛЫ СЕРВЕРА | СБ              | *.snsrv | SQL DB                 |
|  АРХИВ ЖУРНАЛОВ  | ФАЙЛ ЭКСПОРТА   |         | *.omax                 |

  
C:\Program Files\Secret Net Studio\Server\Security Server\Archive\  
при включении трассировки - журнал трассировки C:\logs\SnTrace.log

- Журнал Secret Net Studio:
  - регистрируются все возможные события, кроме некоторых событий категории "Контроль приложений", "Контроль целостности" и "Дискреционный доступ";
  - подробная информация для анализа и контроля работы механизмов;
  - единый формат журналов SNS и Windows;
- Возможность настройки перечня регистрируемых событий и параметров их хранения.
- **Тревоги** – отдельный тип событий высокой степени важности.
- Возможность **квитирования** событий – проставления отметок о прочтении и добавления комментариев к событиям.

## Регистрация событий

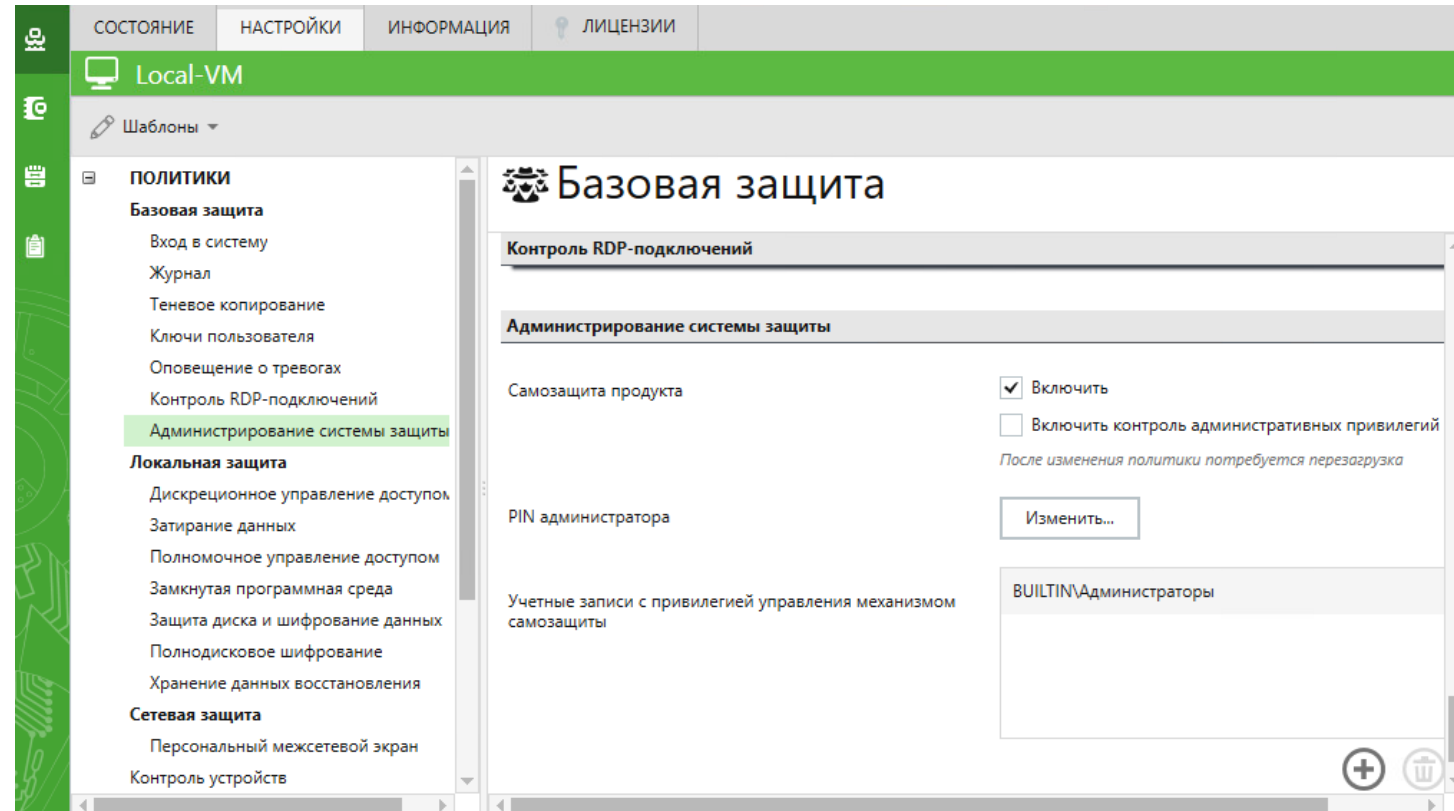
- Журнал Secret Net Studio:
  - регистрируются все возможные события, кроме некоторых событий категории "Контроль приложений", "Контроль целостности" и "Дискреционный доступ";
  - подробная информация для анализа и контроля работы механизмов;
  - единый формат журналов SNS и Windows;
  - Возможность настройки перечня регистрируемых событий и параметров их хранения.
- Тревоги — отдельный тип событий высокой степени важности.
- Возможность квитирования событий — проставления отметок о прочтении и добавления комментариев к событиям.





## Самозащита

- Предотвращение несанкционированной остановки критических служб и процессов.
- Предотвращение выгрузки драйверов Secret Net Studio.
- Обеспечение защиты программных модулей и ключей системного реестра от несанкционированной модификации или удаления.
- Регистрация событий в журнале.



snsshell selfprot deactivatedsd





КС  
без



Контроль целостности

Электронная подпись

ХЭШ ГОСТ 34.11-2012

MD5

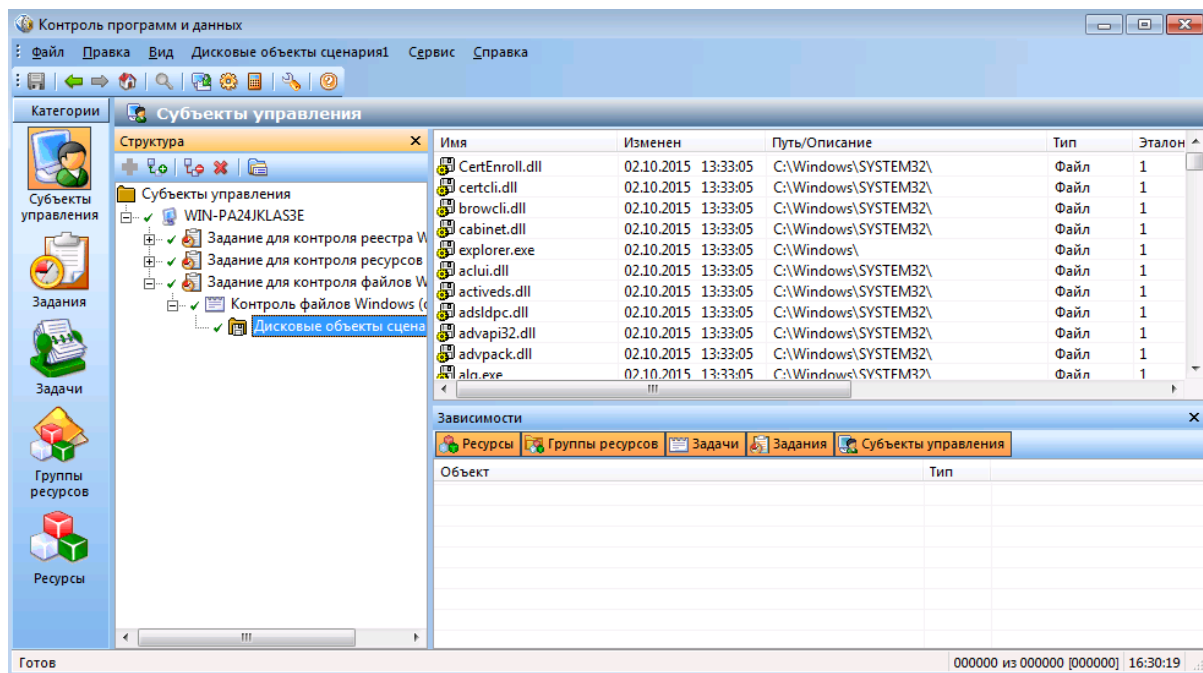
CRC32





## Контроль целостности

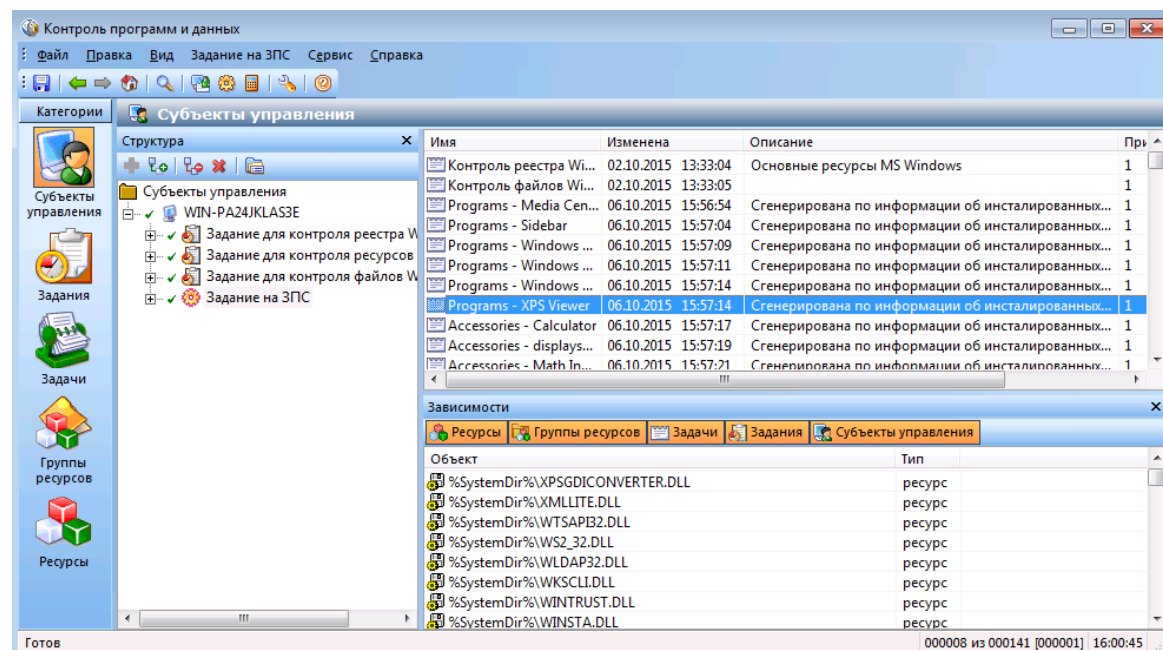
- Возможность контроля файлов, директорий и реестра.
- Алгоритмы – CRC, ЭЦП, хэш, имитовставка, полное совпадение (с восстановлением), встроенная ЭЦП (Microsoft Authenticode).
- Проверка наличия, целостности содержимого, неизменности прав доступа и атрибутов.
- Контроль при загрузке ОС, при входе пользователя, по расписанию.
- Реакция – игнорировать, заблокировать компьютер, восстановить из эталона, восстановить с блокировкой, принять как эталон.
- **Модель данных** – иерархический список объектов с описанием связей между ними, который хранит всю информацию об объектах, методах и расписании контроля.





## Замкнутая программная среда и механизм изоляции процессов

- "Белый" список разрешенных к запуску приложений.
- Автоматическое построение списка разрешенных приложений по ярлыкам из главного меню, событиям журнала и из списка установленных приложений.
- Контроль целостности и неизменности запускаемых приложений.
- Автоматическое построение зависимостей приложений от других бинарных файлов (библиотек и т.д.).
- Контроль скриптов Active Scripts.
- Единая модель данных КЦ-ЗПС.

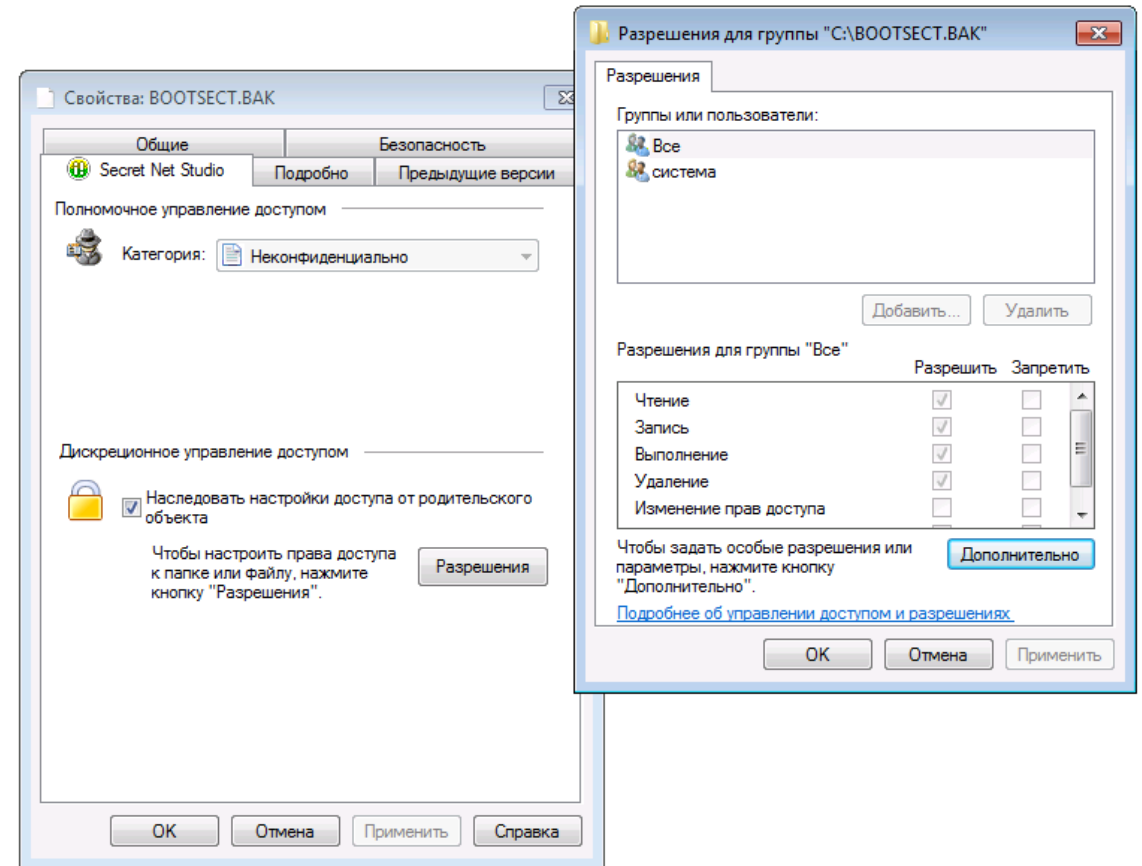






## Дискреционное управление доступом

- Собственные механизмы дискреционного управления доступом, независимые от операционной системы.
- Работа в любой файловой системе, поддерживаемой Windows, включая FAT.
- Унифицированный интерфейс настройки для упрощения перехода к управлению дискреционными правами доступа через Secret Net Studio.
- Дискреционное управление доступом не только к файлам и директориям, но и к устройствам и принтерам.

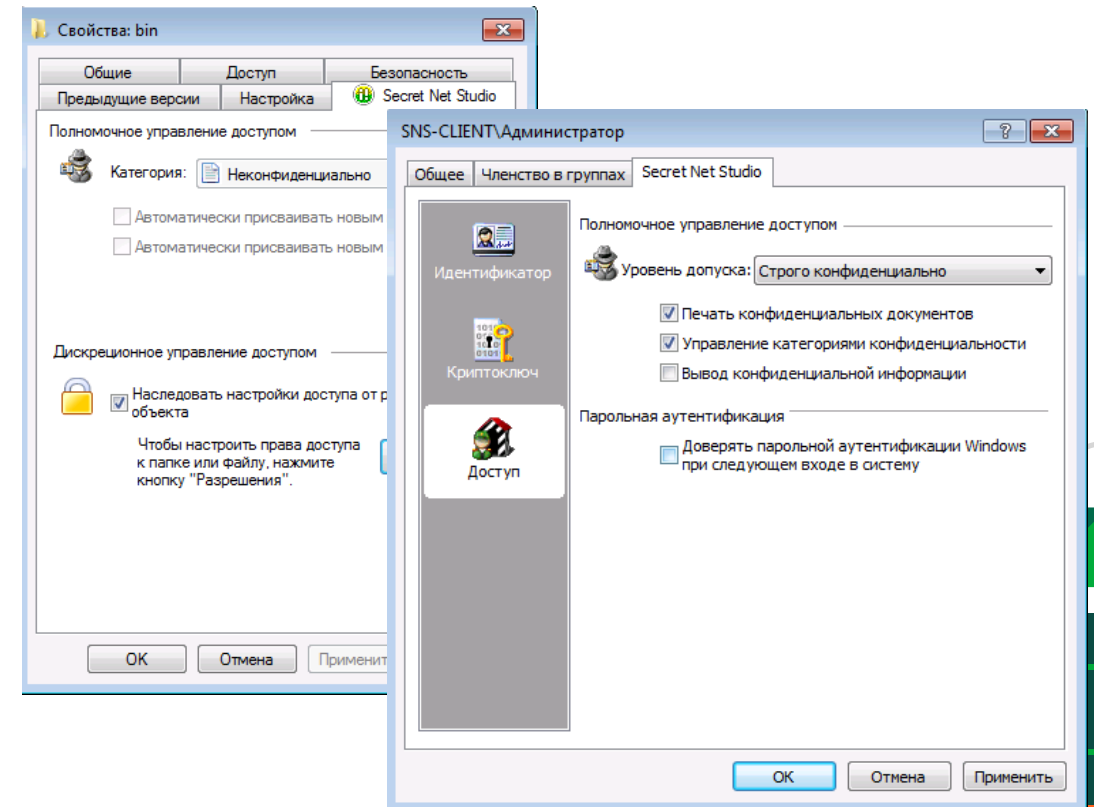






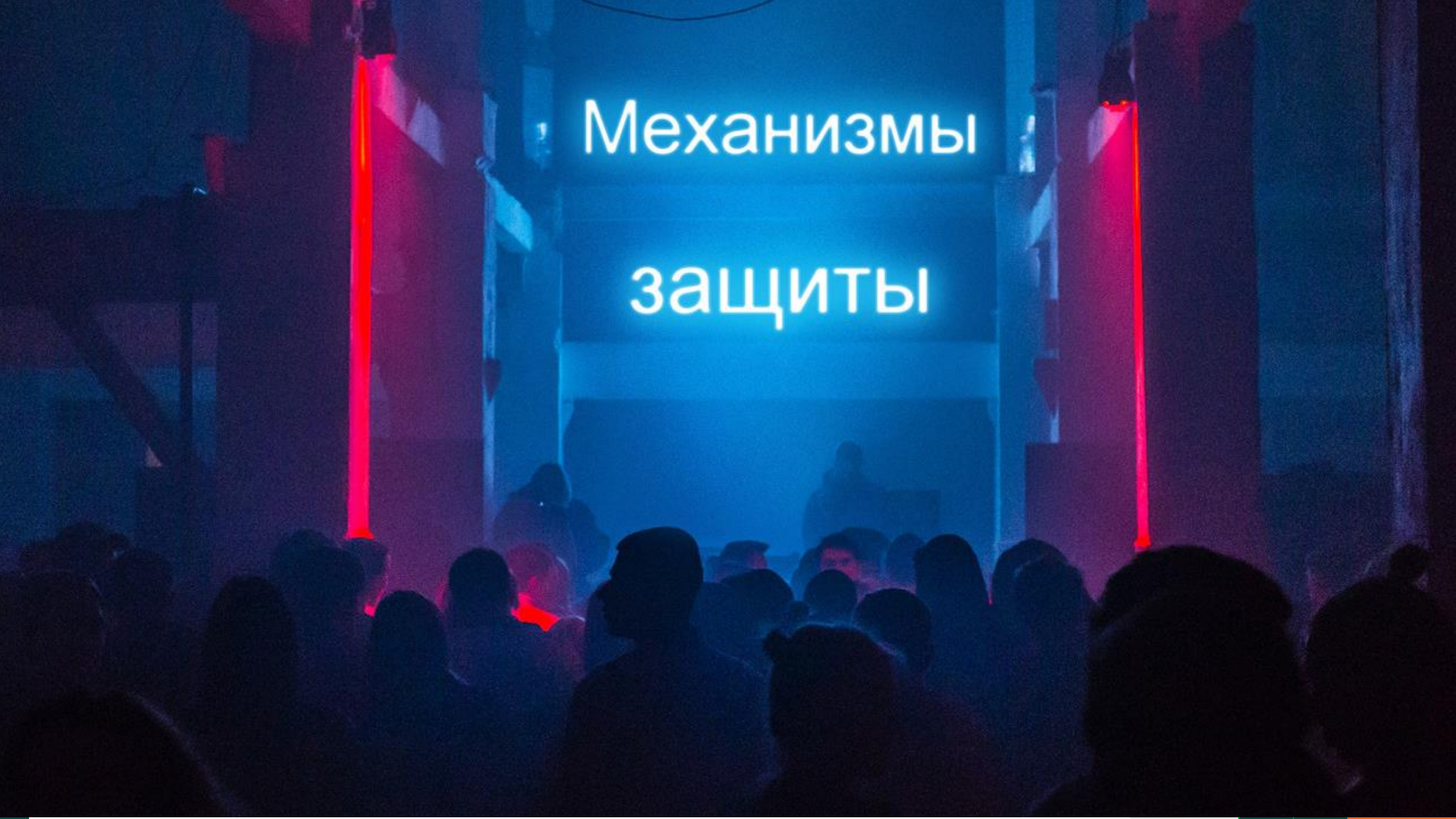
## Полномочное (мандатное) управление доступом

- Назначение мандатных меток через свойства файлов и директорий Windows.
- Настраиваемые метки конфиденциальности и их именование.
- Контроль потоков, возможность строгого контроля терминальных подключений.
- Выбор режима конфиденциальности при входе в систему или автоматическое назначение максимального уровня конфиденциальности.
- Мандатное управление доступом к устройствам и принтерам.



Механизмы

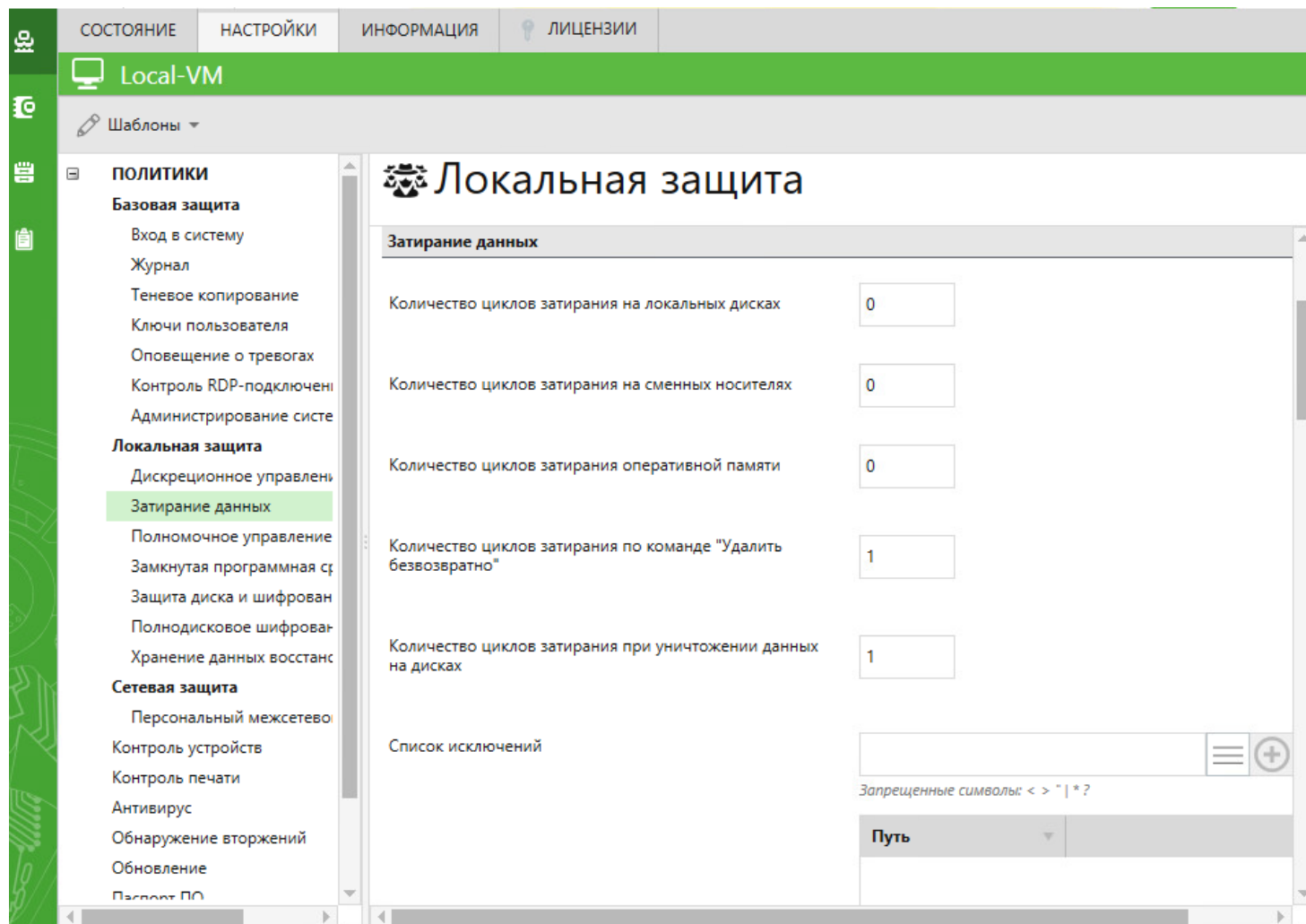
защиты





## Затирание данных

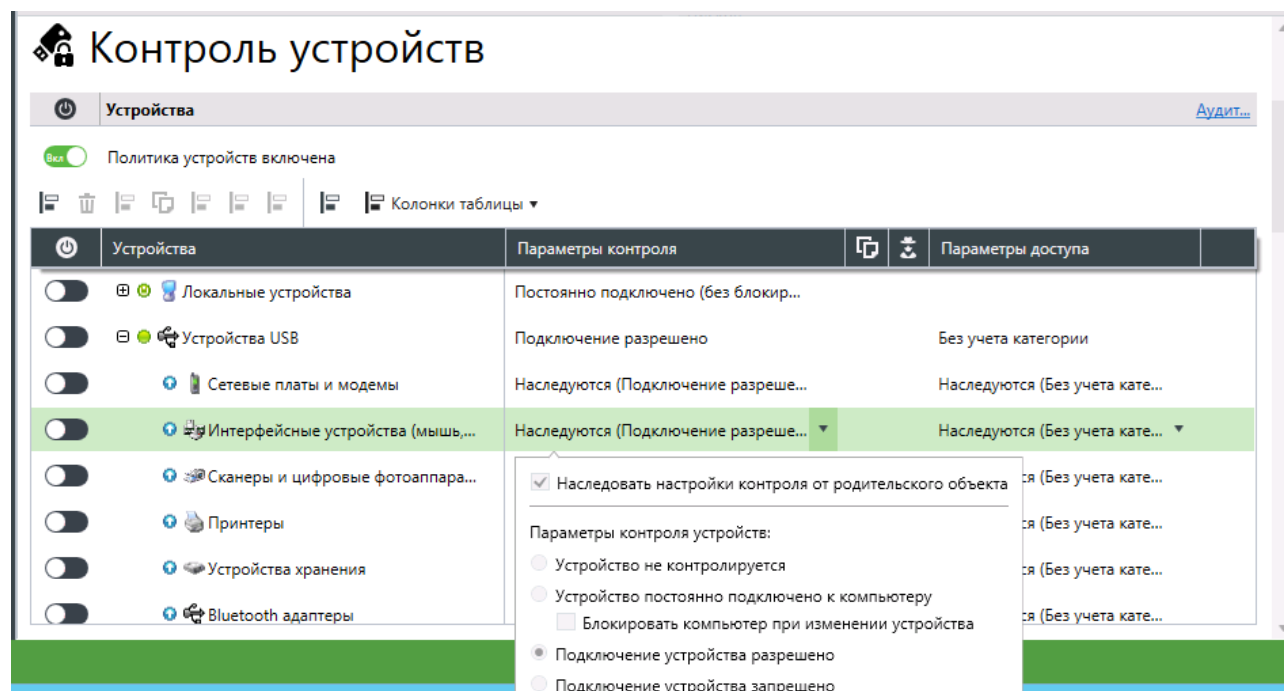
- Автоматическое затирание удаляемой информации.
- Настройка циклов затирания.
- Поддержка файловых систем FAT, NTFS и ReFS.
- Затирание информации на локальных и сменных носителях.
- Работа в оперативной памяти, исключая повторное использование конфиденциальной информации или ПД пользователей после завершения работы программных процессов и при любых операциях освобождения виртуальной памяти.





## Контроль устройств

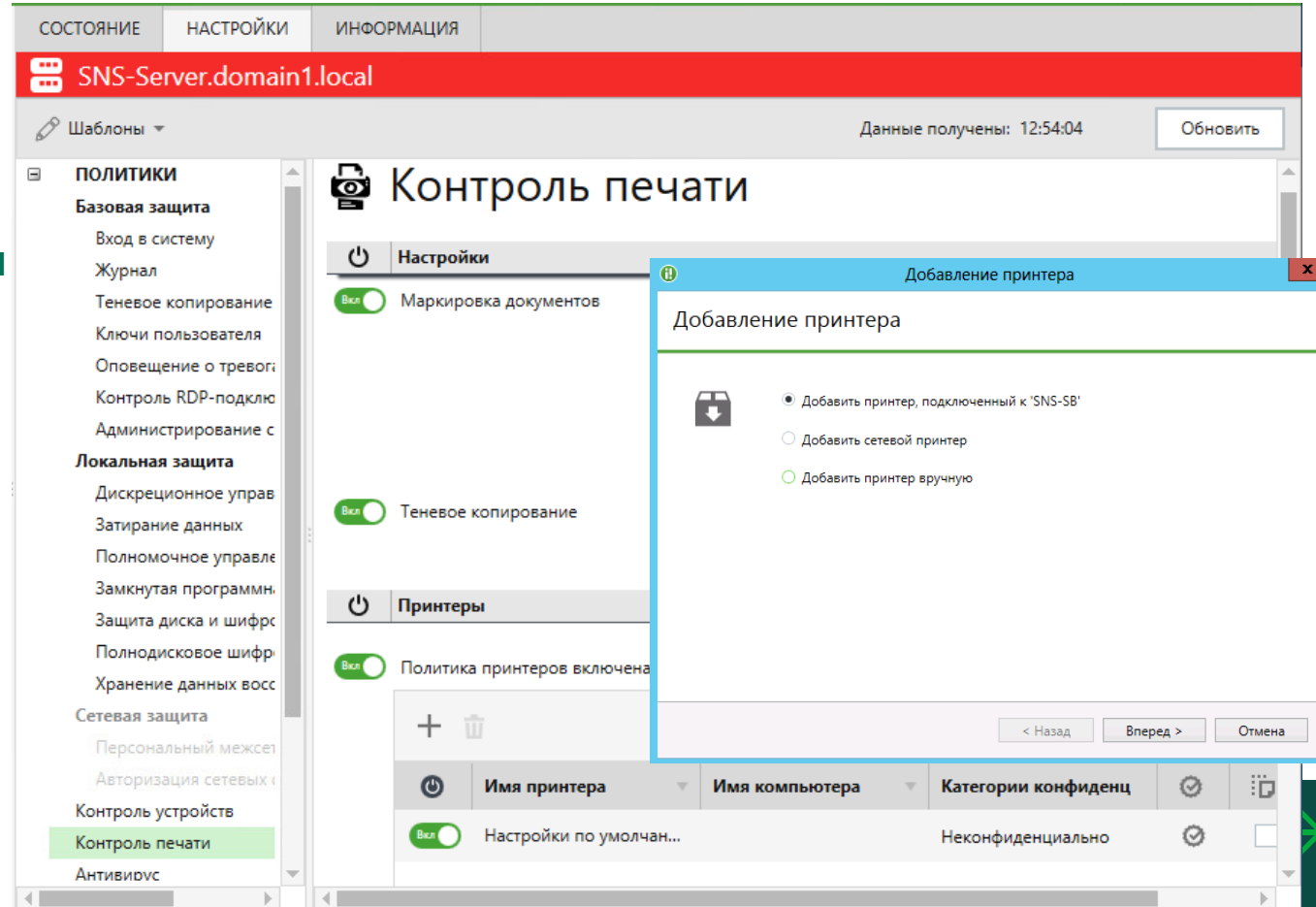
- Контроль осуществляется по группам, классам, моделям и отдельным устройствам.
- Иерархическое наследование настроек.
- Дискреционное и полномочное управление доступом.
- Возможность контроля подключений и отключений устройств.
- Возможность блокировки компьютера при изменении аппаратной конфигурации.
- Согласование изменения аппаратной конфигурации у администратора.
- Управление перенаправлением устройств в терминальных подключениях.





## Контроль печати

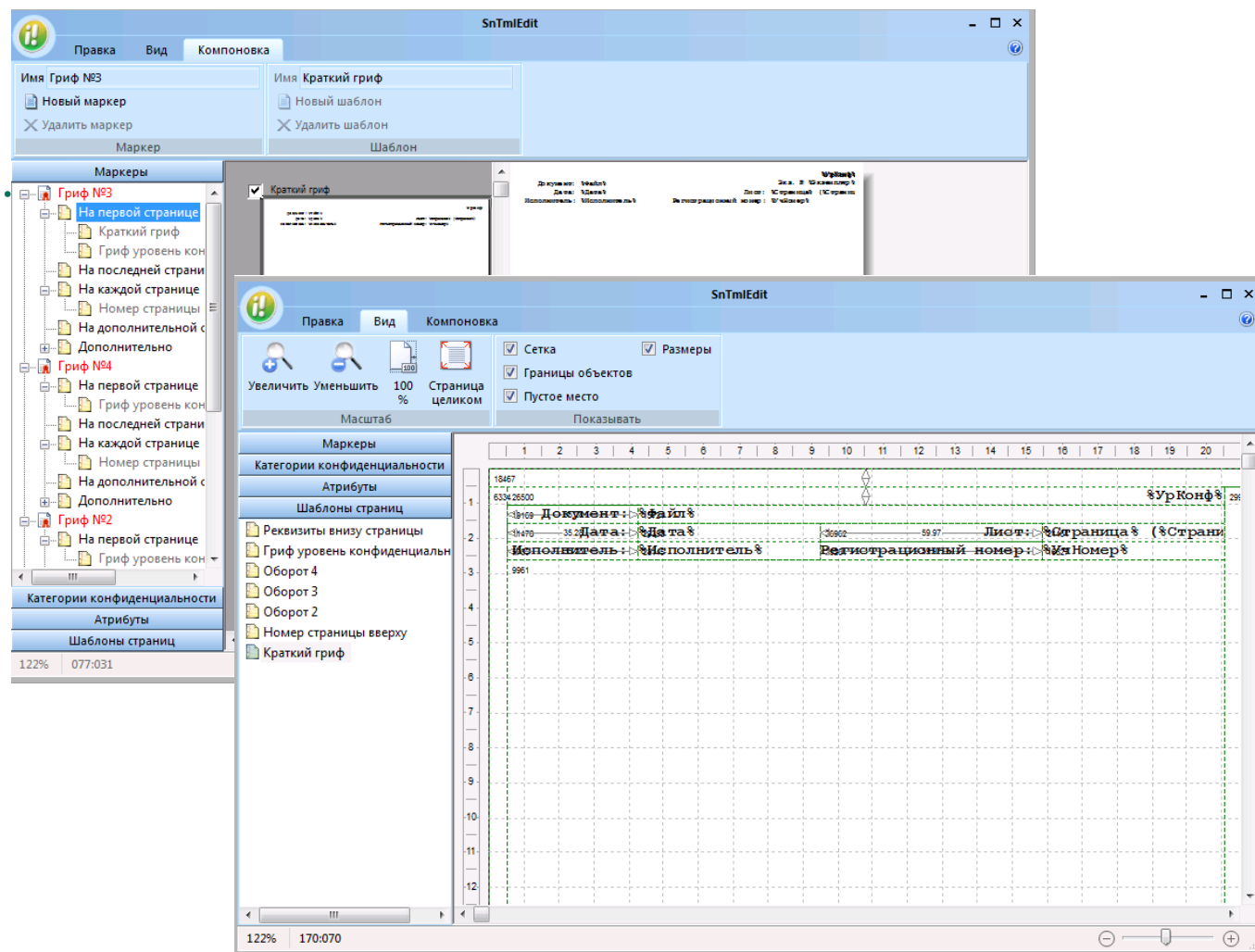
- Настройка отдельных принтеров и правила для всех подключенных устройств.
- Поддержка виртуальных принтеров.
- Дискреционное и полномочное управление доступом.
- Возможность ограничения уровня конфиденциальности документов для печати.





## Маркировка документов

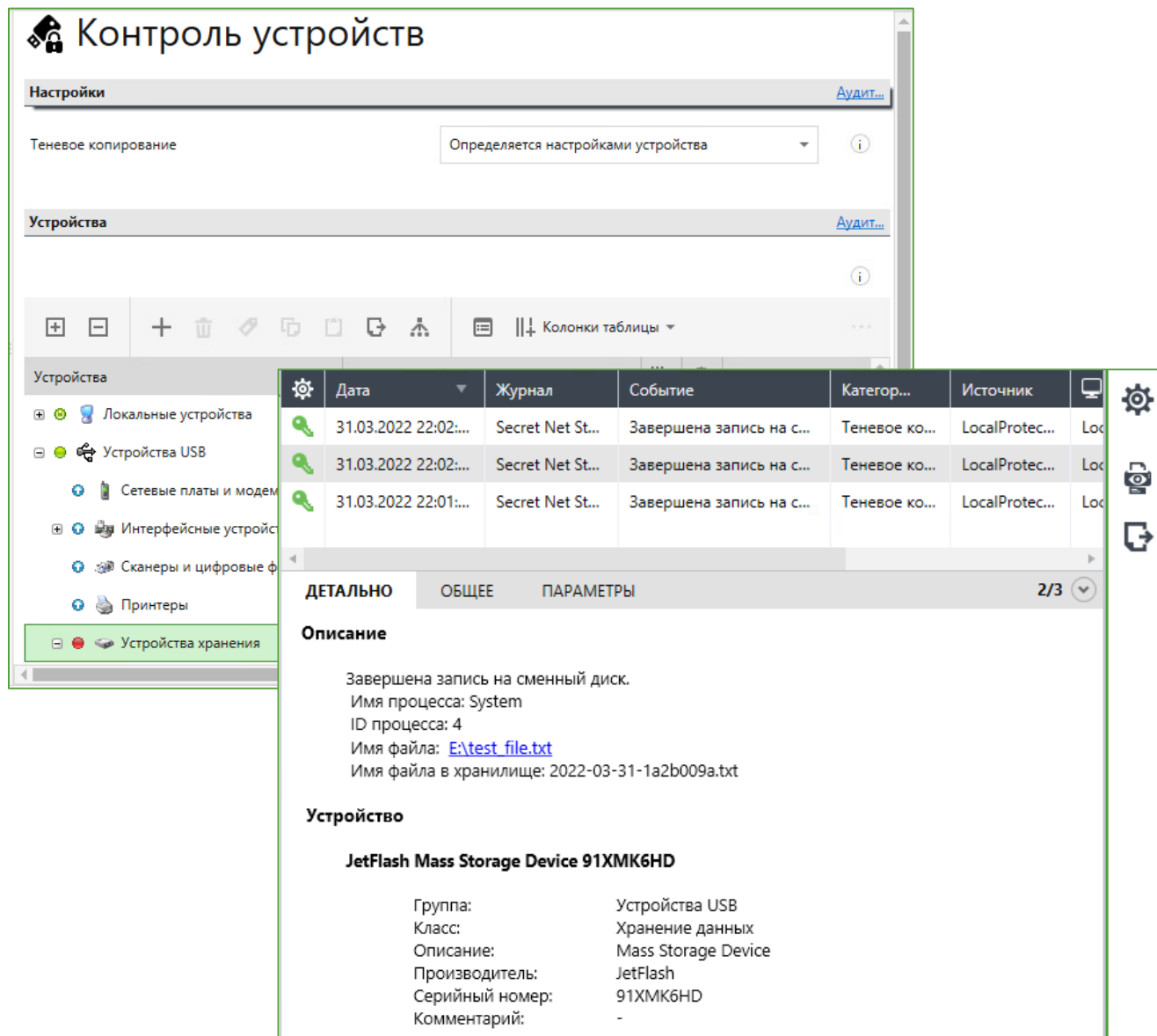
- Маркировка выводимых на печать документов.
- Разные маркеры в зависимости от уровня конфиденциальности документа.
- Полностью настраиваемые маркеры с возможностью добавления произвольных полей.
- Отдельные маркеры для первой и последней страниц.





## Теневое копирование

- Теневое копирование файлов, выводимых на съемные носители.
- Теневое копирование распечатываемых документов.
- Локальное управление теневыми копиями.
- Хранение теневых копий в защищенном хранилище.
- Возможность расследования инцидентов, связанных с утечками информации.
- Контроль заполнения теневого хранилища с возможностью циклической перезаписи.



**Контроль устройств**

Настройки [Аудит...](#)

Теневое копирование: Определяется настройками устройства [i](#)

Устройства [Аудит...](#)

Устройства

| Устройства            | Дата                 | Журнал           | Событие                  | Категор...    | Источник       |     |
|-----------------------|----------------------|------------------|--------------------------|---------------|----------------|-----|
| Локальные устройства  | 31.03.2022 22:02:... | Secret Net St... | Завершена запись на с... | Теневое ко... | LocalProtec... | Loc |
| Устройства USB        | 31.03.2022 22:02:... | Secret Net St... | Завершена запись на с... | Теневое ко... | LocalProtec... | Loc |
| Сетевые платы и модем | 31.03.2022 22:01:... | Secret Net St... | Завершена запись на с... | Теневое ко... | LocalProtec... | Loc |
| Интерфейсные устройс  |                      |                  |                          |               |                |     |
| Сканеры и цифровые ф  |                      |                  |                          |               |                |     |
| Принтеры              |                      |                  |                          |               |                |     |
| Устройства хранения   |                      |                  |                          |               |                |     |

ДЕТАЛЬНО ОБЩЕЕ ПАРАМЕТРЫ 2/3

**Описание**

Завершена запись на сменный диск.  
Имя процесса: System  
ID процесса: 4  
Имя файла: [E:\test\\_file.txt](#)  
Имя файла в хранилище: 2022-03-31-1a2b009a.txt

**Устройство**

**JetFlash Mass Storage Device 91XMK6HD**

|                 |                     |
|-----------------|---------------------|
| Группа:         | Устройства USB      |
| Класс:          | Хранение данных     |
| Описание:       | Mass Storage Device |
| Производитель:  | JetFlash            |
| Серийный номер: | 91XMK6HD            |
| Комментарий:    | -                   |



## Теневое копирование

Теневую копию можно получить ТОЛЬКО локально, следующими методами:

- 1) Из локального ЦУ через запись журнала о сохранении Теневой Копии (по ссылке)
- 2) Из папки хранения теневой копии.

При ТК для печати – поток печати сохраняется в файл формата \*.xps.

(при этом, ТК не включает в себя маркеры)

При ТК для файлов, копируемых на внешние устройства – формат файла не меняется, но он переименовывается по формуле:

*дата-номер\_объекта\_ТК.оригинальное\_расширение\_файла*

Сохранение ТК происходит в следующих папках:

Файл ТК печати:

C:\System Volume Information\SnCloneVault\PRINT\SSID\_пользователя\дата-номер\_объекта\_ТК.xps

Файл ТК на внешние устройства:

C:\System Volume Information\SnCloneVault\FILE\SSID\_пользователя\дата-номер\_объекта\_ТК.оригинальное\_расширение

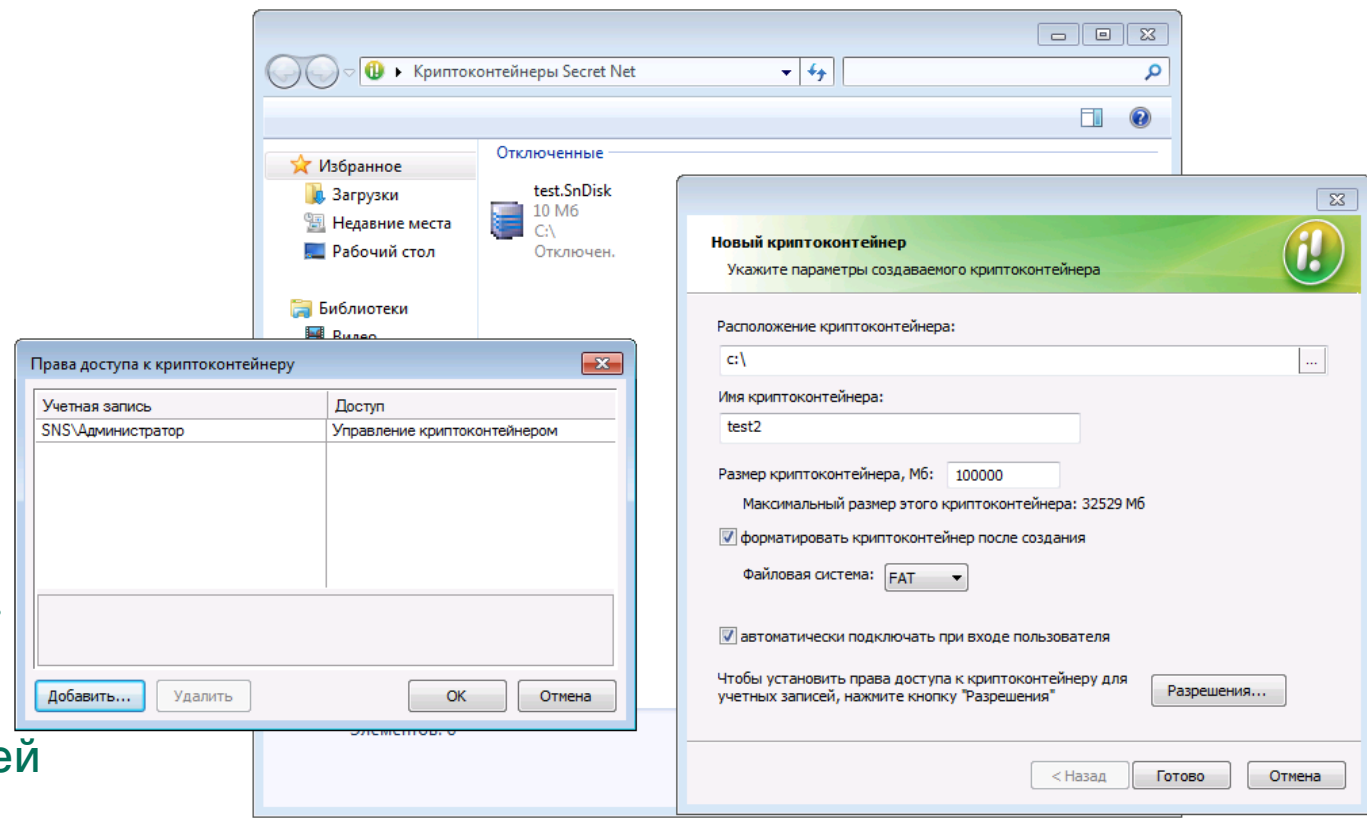


Шифрование



## Шифрование данных

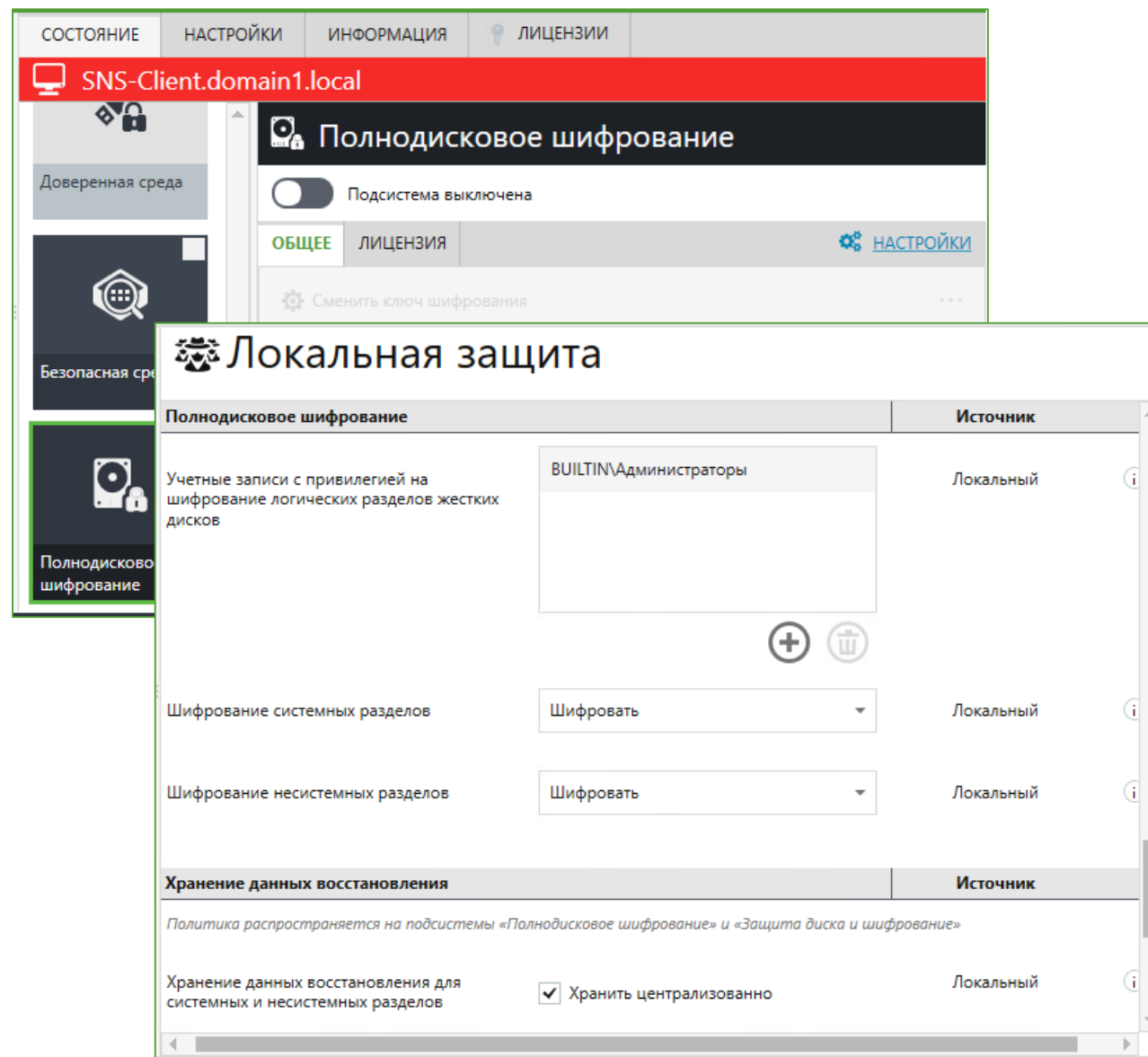
- Зашифрованные контейнеры: физически — файл на диске, логически — подключаемый виртуальный жесткий диск, вся информация на котором зашифрована.
- Хранение ключевой информации — на электронных ключах или съемных дисках (флешки, дискеты).
- Произвольный размер контейнеров.
- Возможность автоматического подключения.
- Настраиваемые права доступа.
- Возможность резервного копирования ключей шифрования.





## Полнодисковое шифрование

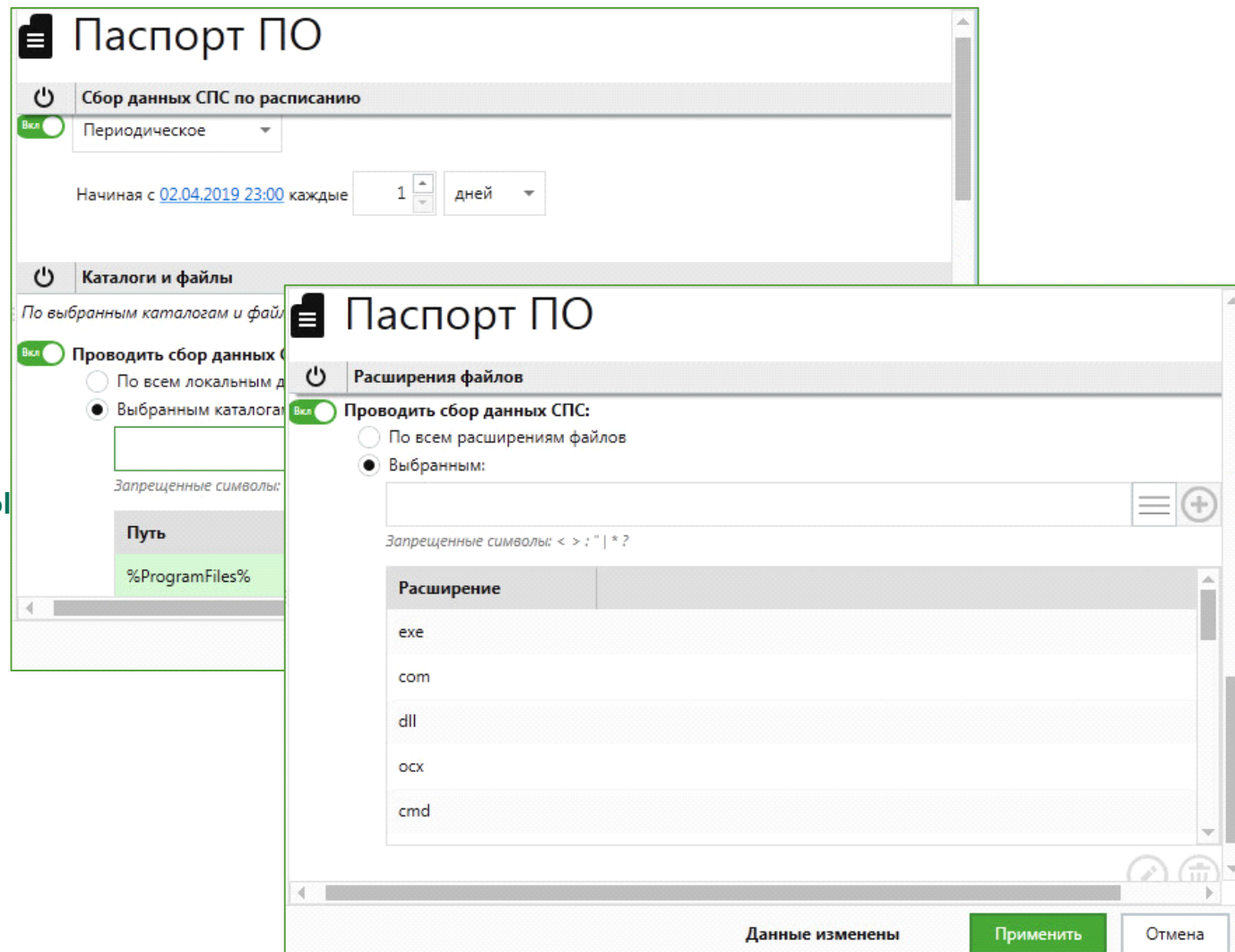
- Шифрование данных на носителях информации для предотвращения попыток НСД к конфиденциальной информации.
- Поддержка системных и несистемных разделов жестких дисков со структурой GPT и режимом загрузки UEFI.
- Поддержка шифрования несистемных разделов жестких дисков со структурой MBR.
- Алгоритм шифрования — AES-256. Ключевая информация хранится в зашифрованном виде на незашифрованном разделе ESP.
- Для доступа к зашифрованным дискам необходимо ввести пароль, установленный при шифровании данных.





## Паспорт ПО

- Предназначен для контроля состава и целостности ПО, установленного на защищаемых компьютерах.
- Распознавание исполняемых файлов.
- Сканирование: периодически по расписанию или в произвольные моменты времени по команде пользователя.
- Полученные в результате сканирования данные сравниваются с результатами предыдущего сканирования.
- Утверждение данных сканирования в качестве текущего паспорта.



**Паспорт ПО**

Сбор данных СПС по расписанию

Вкл ☐ Периодическое

Начиная с 02.04.2019 23:00 каждые  дней

**Каталоги и файлы**

По выбранным каталогам и файлам

Вкл ☐ Проводить сбор данных СПС:

☐ По всем локальным дискам

☒ Выбранным каталогам

Запрещенные символы:

Путь

%ProgramFiles%

**Расширения файлов**

Вкл ☐ Проводить сбор данных СПС:

☐ По всем расширениям файлов

☒ Выбранным:

Запрещенные символы: < > : " | \* ?

| Расширение |
|------------|
| exe        |
| com        |
| dll        |
| ocx        |
| cmd        |

Данные изменены



## Межсетевой экран

- Фильтрация на сетевом уровне с независимым принятием решений по каждому пакету.
- Фильтрация пакетов служебных протоколов (ICMP, IGMP и т.д.) для диагностики и управления работой сетевых устройств.
- Фильтрация с учетом входного и выходного сетевого интерфейса для проверки подлинности сетевых адресов.
- Фильтрация на транспортном уровне запросов на установление TCP-сессий.
- Фильтрация на прикладном уровне запросов к прикладным сервисам (фильтрация по символьной последовательности в пакетах).
- Фильтрация с учетом полей сетевых пакетов.
- Фильтрация с учетом даты/времени суток.

### Защита сетевых подключений

#### Межсетевой экран

Правила доступа

Правила, регламентирующие доступ к [сетевым сервисам](#) (TCP/IP v4) данного компьютера.

| Вкл                                 | Субъект  | Сетевой сер   | Тип доступа | Направление | Удаленный | Прилож |
|-------------------------------------|----------|---------------|-------------|-------------|-----------|--------|
| <input checked="" type="checkbox"/> | anonymou | DNS-запрос    | Разрешен    | Исходящее   | *         | *      |
| <input checked="" type="checkbox"/> | anonymou | DHCP-ответ    | Разрешен    | Входящее    | *         | *      |
| <input checked="" type="checkbox"/> | anonymou | DHCP-запрос   | Разрешен    | Исходящее   | *         | *      |
| <input checked="" type="checkbox"/> | anonymou | NetBIOS (служ | Разрешен    | Входящее    | *         | *      |
| <input checked="" type="checkbox"/> | anonymou | NetBIOS (служ | Разрешен    | Входящее    | *         | *      |

[Показать специализированные правила доступа](#)

Системные правила: 0  
Прикладные правила: 0

#### Настройки

##### Протоколы

| Протокол                            | Доступ                              | Аудит                    | По умолчанию |
|-------------------------------------|-------------------------------------|--------------------------|--------------|
| Internet Protocol, version 4 (IPv4) | <input checked="" type="checkbox"/> | <input type="checkbox"/> |              |
| Internet Protocol, version 6 (IPv6) | <input type="checkbox"/>            | <input type="checkbox"/> |              |

##### Разрешить следующие типы ICMP-сообщений:

| Описание                        | Тип | Код   | Получение                           | Отправка                            |
|---------------------------------|-----|-------|-------------------------------------|-------------------------------------|
| Эхо-ответ                       | 0   | Любой | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| Адресат недоступен              | 3   | Любой | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Перенаправление                 | 5   | Любой | <input type="checkbox"/>            | <input type="checkbox"/>            |
| Альтернативный адрес узла       | 6   | Любой | <input type="checkbox"/>            | <input type="checkbox"/>            |
| Эхо-запрос                      | 8   | Любой | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| Ходатайство маршрутизатора      | 10  | Любой | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Превышение временного интервала | 11  | Любой | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |

☐ Заблокировать остальные типы ICMP-сообщений

#### Свойства правила доступа

ОБЩИЕ ДОПОЛНИТЕЛЬНО РАСПИСАНИЕ

Доступ: ☒ Разрешить  
☐ Запретить

Сетевой сервис:

Направление:  [Редактировать](#)

Протокол:

Локальный порт:

Удаленный порт:

Приложение:  [Редактировать](#)

Пользователь:  [Выбрать](#)

☐ Отключить правило

☐ Уведомлять отправителя о блокировке пакета

#### Свойства правила доступа

ОБЩИЕ ДОПОЛНИТЕЛЬНО РАСПИСАНИЕ

☒ Задать расписание

|       | Понедель | Вторник | Среда | Четверг | Пятница | Суббота | Воскресе |
|-------|----------|---------|-------|---------|---------|---------|----------|
| 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 |          |         |       |         |         |         |          |

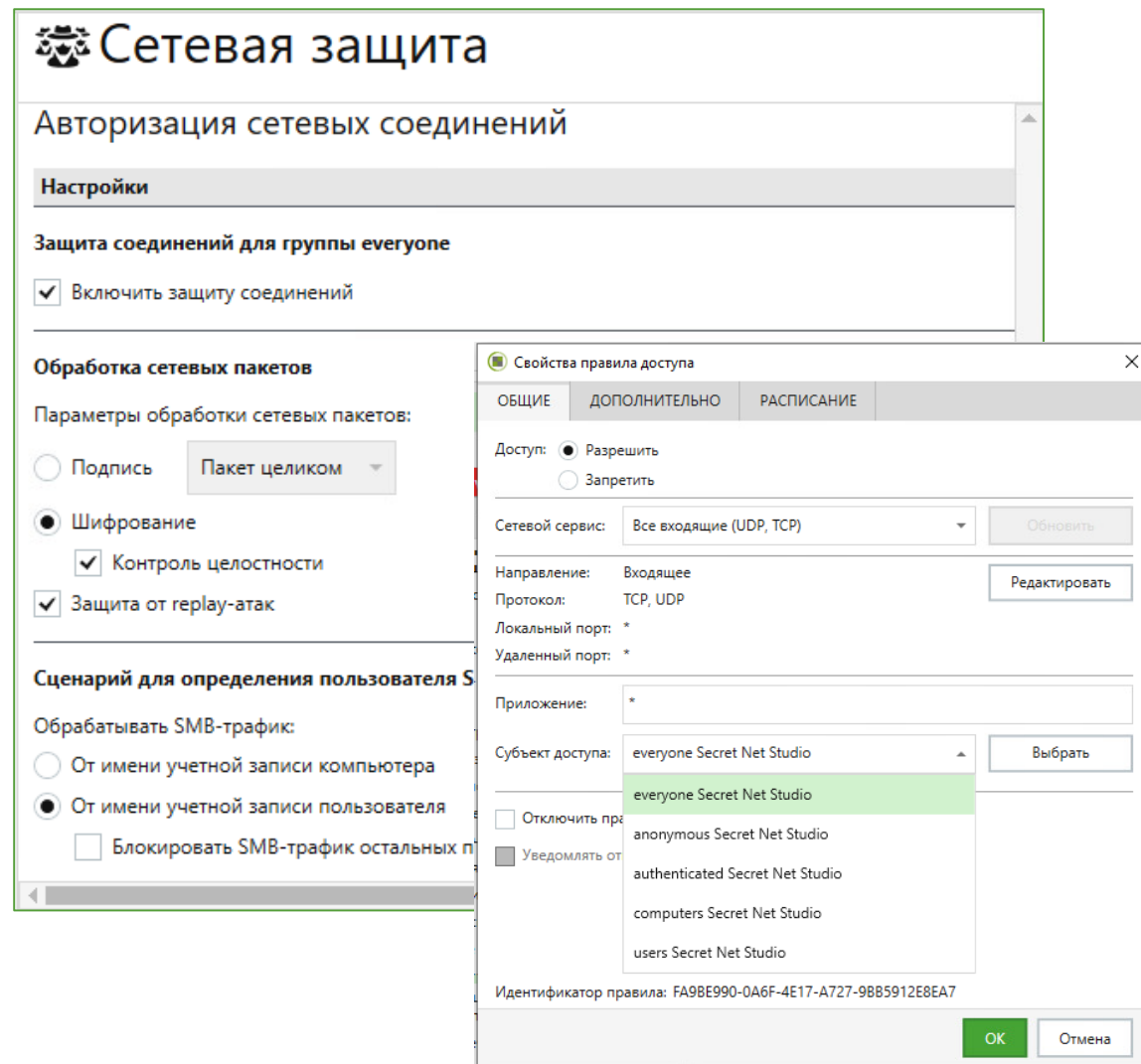
Правило: ☒ активно ☐ не активно

[Применить](#) [Отмена](#)



## Авторизация сетевых соединений

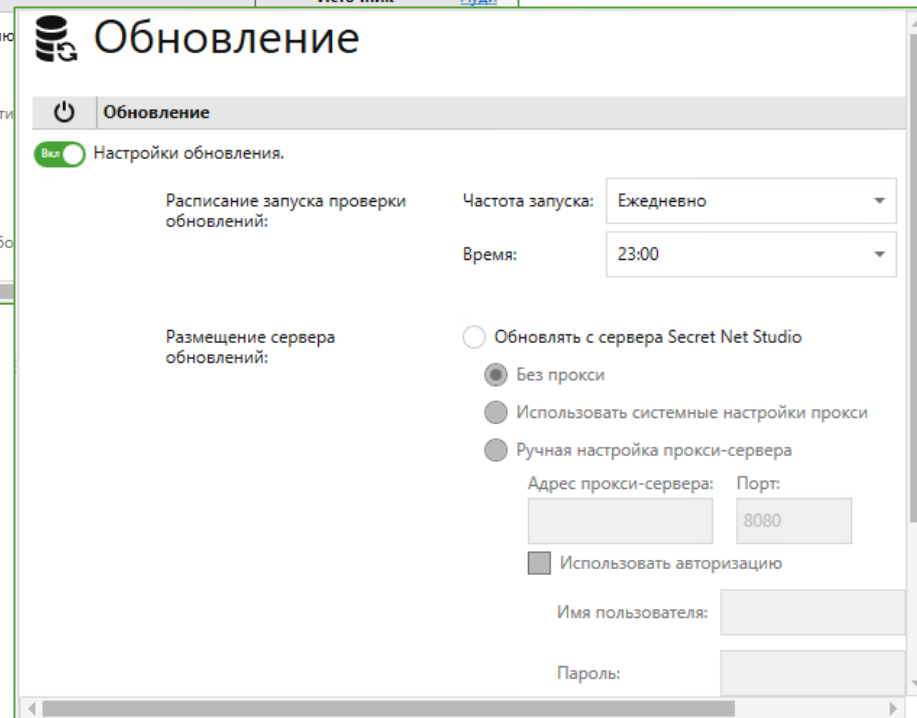
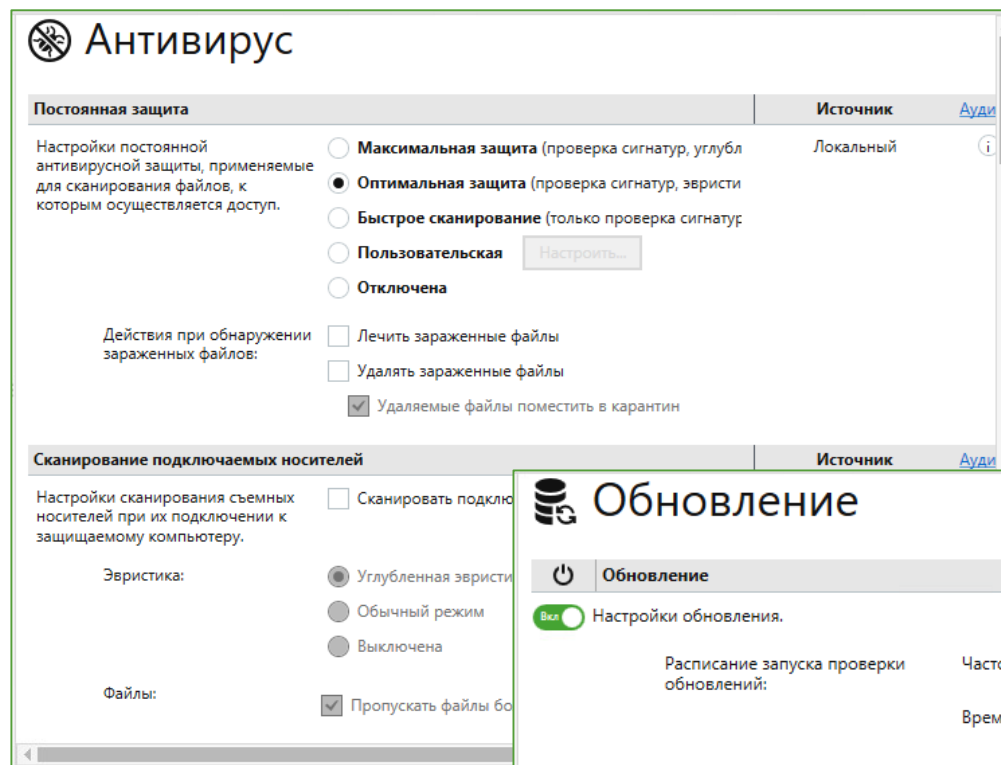
- Технологии Kerberos и IPSec, защита от атак типа Man in the middle.
- Возможность использовать конкретных пользователей и группы пользователей в правилах межсетевого экрана — как во входящих, так и в исходящих.
- Поддержка гибкого разграничения сетевого доступа для терминальных серверов.
- Возможность реализовать программные VLAN'ы.
- Возможность сокрытия сетевого трафика (кодирование информации).





## Антивирус

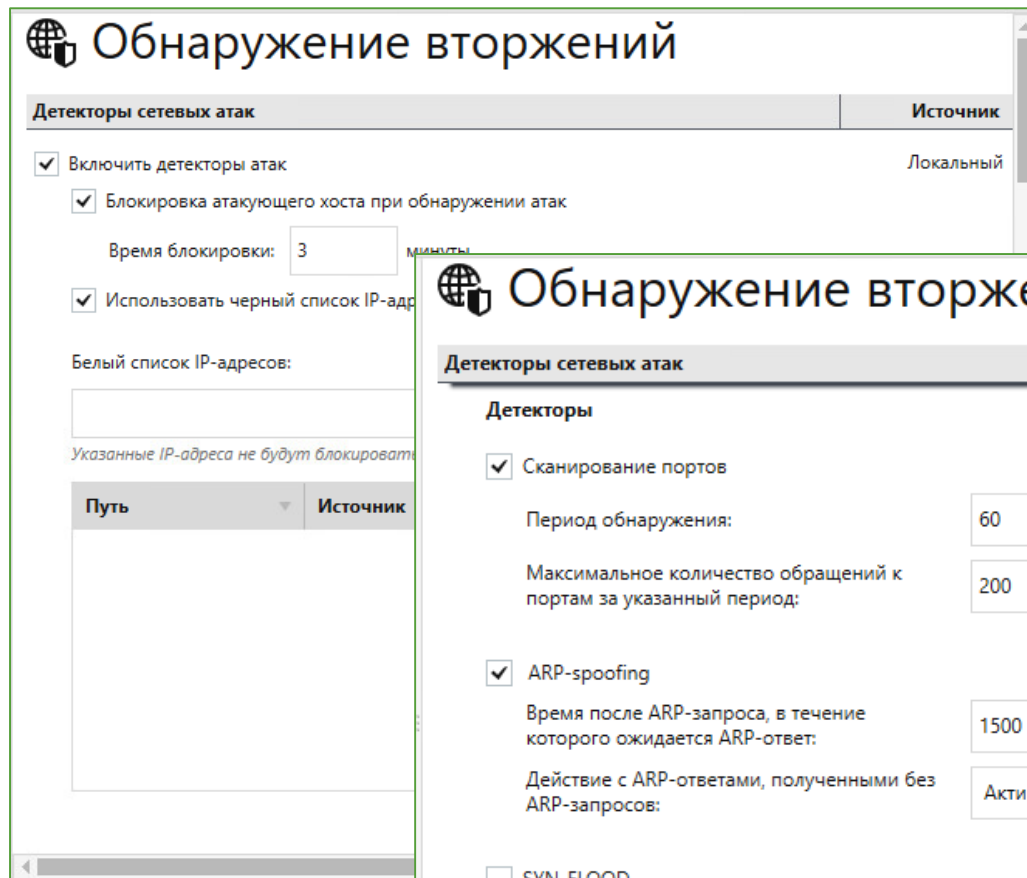
- Использование одного из компонентов:
  - Антивирус SNS;
  - Антивирус Касперский.
- Высокая скорость работы, отличные показатели обнаружения и отсутствия ложных срабатываний.
- Сигнатурные и эвристические методы контроля.
- Поддержка «белых» списков директорий и файлов.
- Различные профили сканирования, возможность контекстного сканирования из «Проводника».
- Возможность развертывания локальных серверов обновлений с поддержкой каскадных режимов работы.





## Защита от вторжений

- Эвристические детекторы сетевых атак — сканирование портов, атаки типа Denial of Service, аномальный сетевой трафик и т.д.
- Сигнатурные детекторы атак.
- Возможность временной блокировки атакующих компьютеров.
- Наличие команды оперативного снятия блокировки.



Обнаружение вторжений

Детекторы сетевых атак

Источник: Локальный

☒ Включить детекторы атак

☒ Блокировка атакующего хоста при обнаружении атак

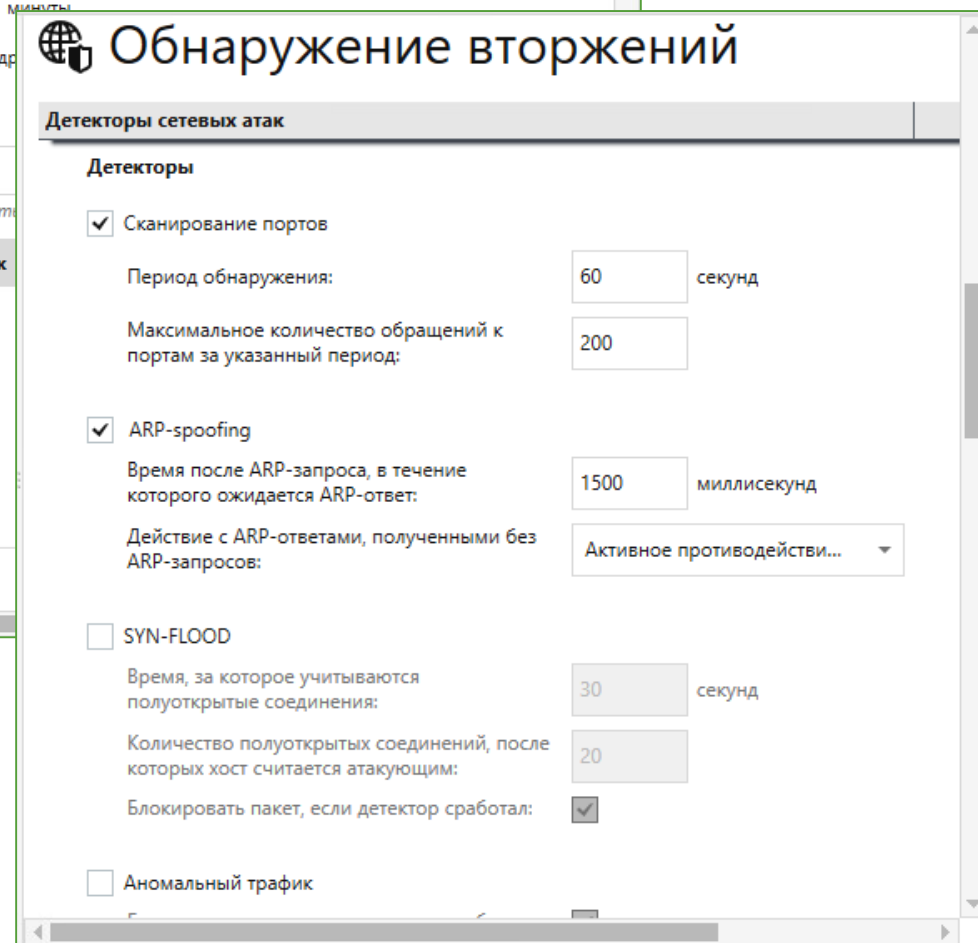
Время блокировки: 3 минуты

☒ Использовать черный список IP-адресов

Белый список IP-адресов:

Указанные IP-адреса не будут блокироваться

| Путь | Источник |
|------|----------|
|------|----------|



Обнаружение вторжений

Детекторы сетевых атак

Детекторы

☒ Сканирование портов

Период обнаружения: 60 секунд

Максимальное количество обращений к портам за указанный период: 200

☒ ARP-spoofing

Время после ARP-запроса, в течение которого ожидается ARP-ответ: 1500 миллисекунд

Действие с ARP-ответами, полученными без ARP-запросов: Активное противодействие...

☐ SYN-FLOOD

Время, за которое учитываются полуоткрытые соединения: 30 секунд

Количество полуоткрытых соединений, после которых хост считается атакующим: 20

Блокировать пакет, если детектор сработал: ☒

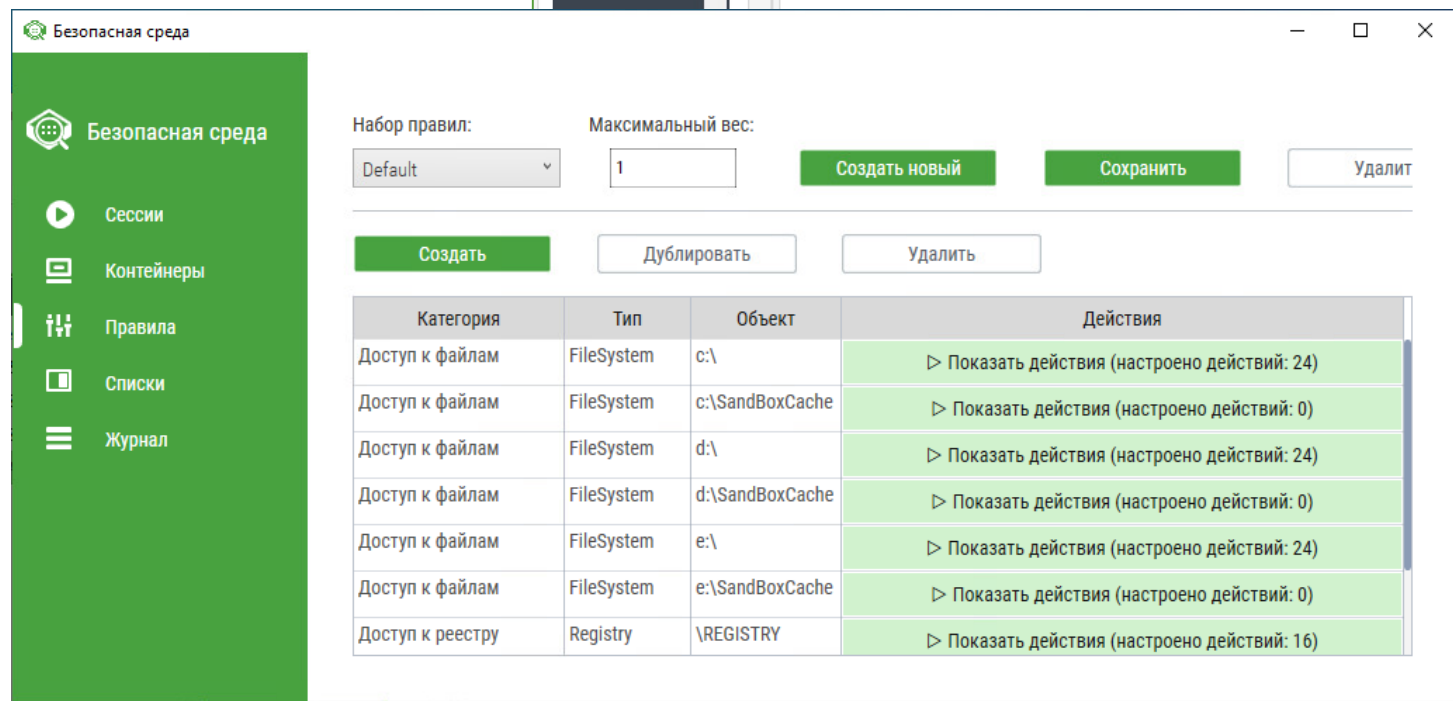
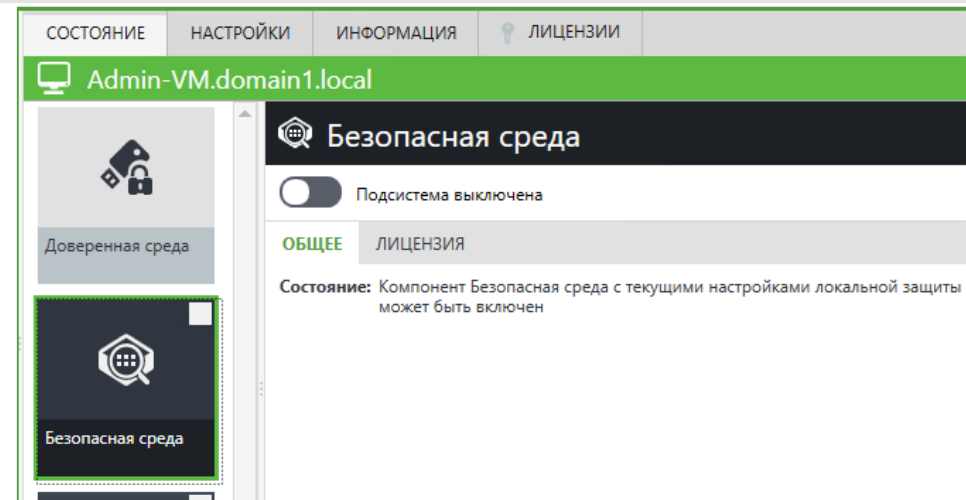
☐ Аномальный трафик



## Безопасная (изолированная) среда

Предотвращение нанесения ущерба ресурсам защищаемого компьютера путем

- запуска неизвестного программного обеспечения в изолированной среде;
- анализа работы неизвестного ПО на основе специальных правил;
- определения уровня доверия и на его основании добавления исследуемой программы либо в список доверенных (белый), либо в список запрещенных (черный).





## Доверенная среда

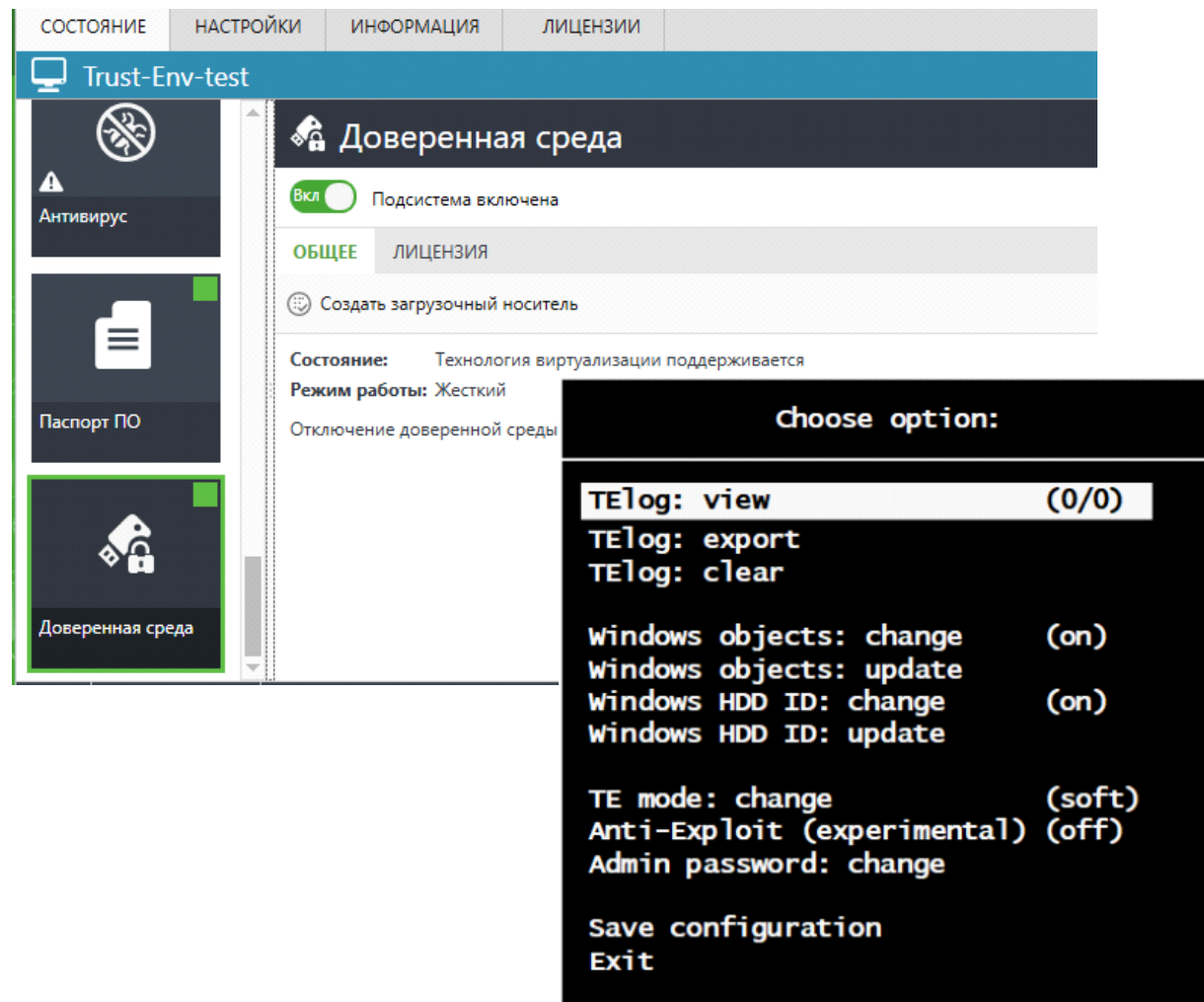
- Контроль целостности файлов до загрузки ОС.
- Контроль запуска и работы модулей SNS (драйверов, служб, приложений) и других драйверов.
- Контроль подлинности системного диска.
- Блокировка от записи страниц памяти, в которых размещаются модули SNS и другие драйверы.
- Обнаружение компьютерных атак, их предотвращение или аварийное завершение работы ОС.
- Регистрация событий в журнале.

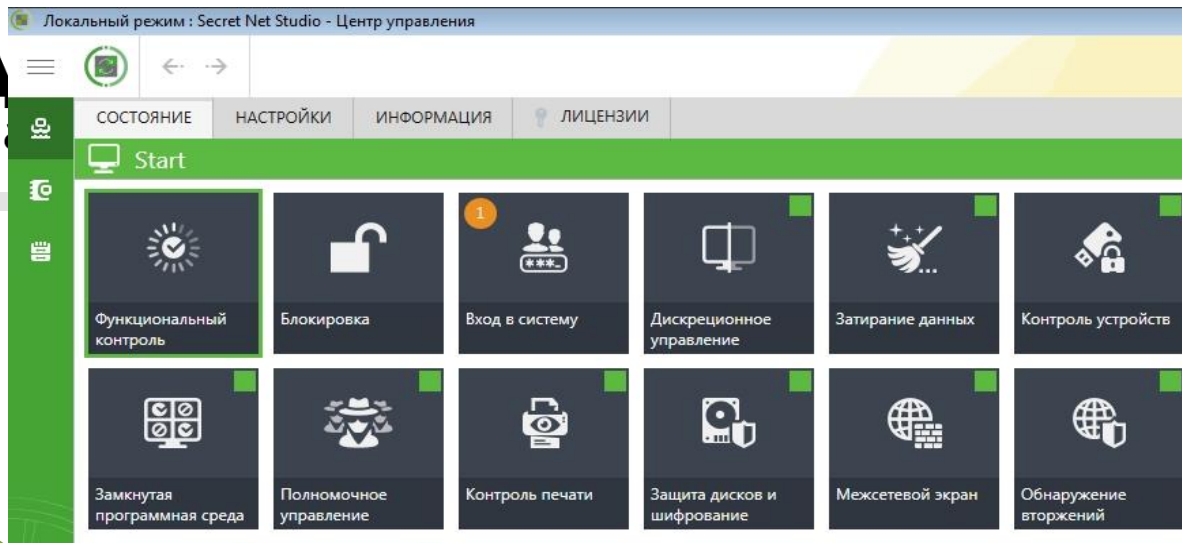
### Загрузочный носитель ДС:

- специализированная ОС ДС на базе ОС Linux;
- гипервизор ДС, обеспечивающий загрузку ОС ДС;
- загрузчик ДС (MBR или UEFI).

### Обнаружение компьютерных атак.

### Настройки ДС.

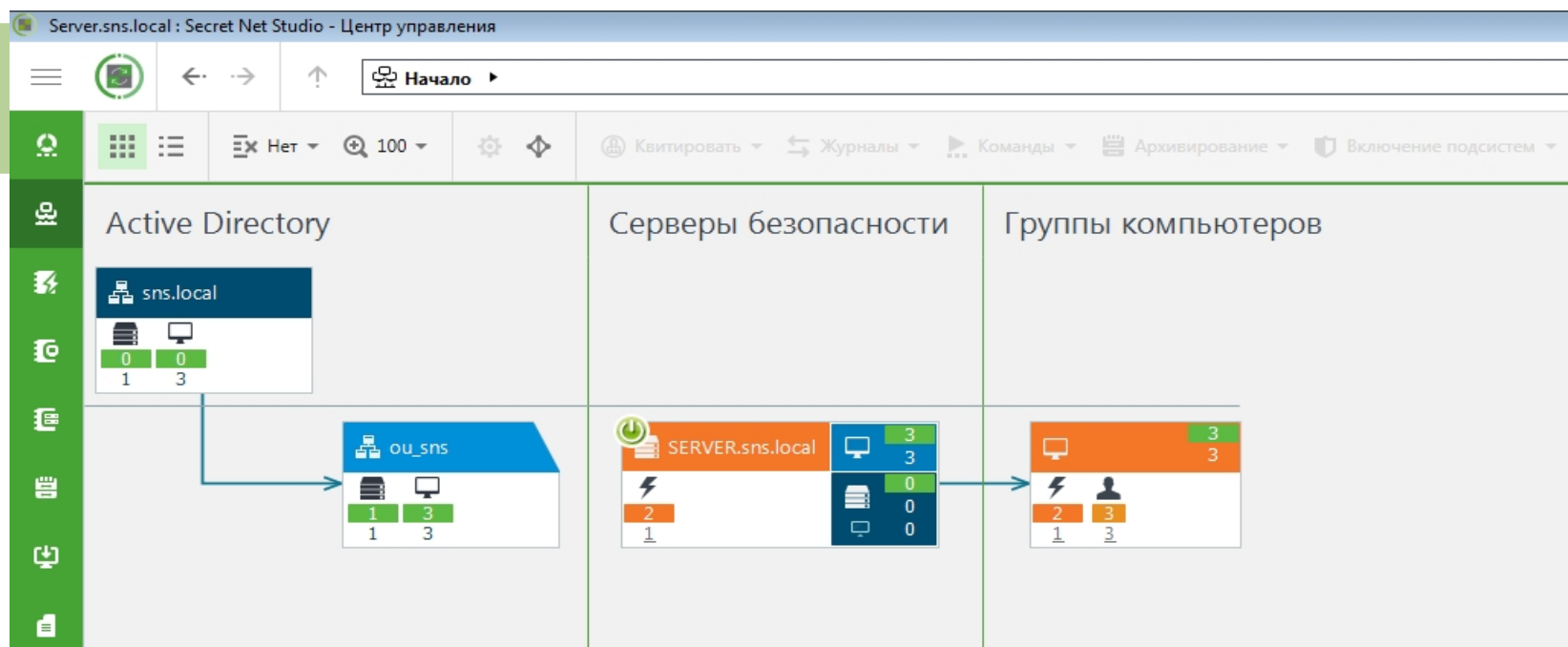




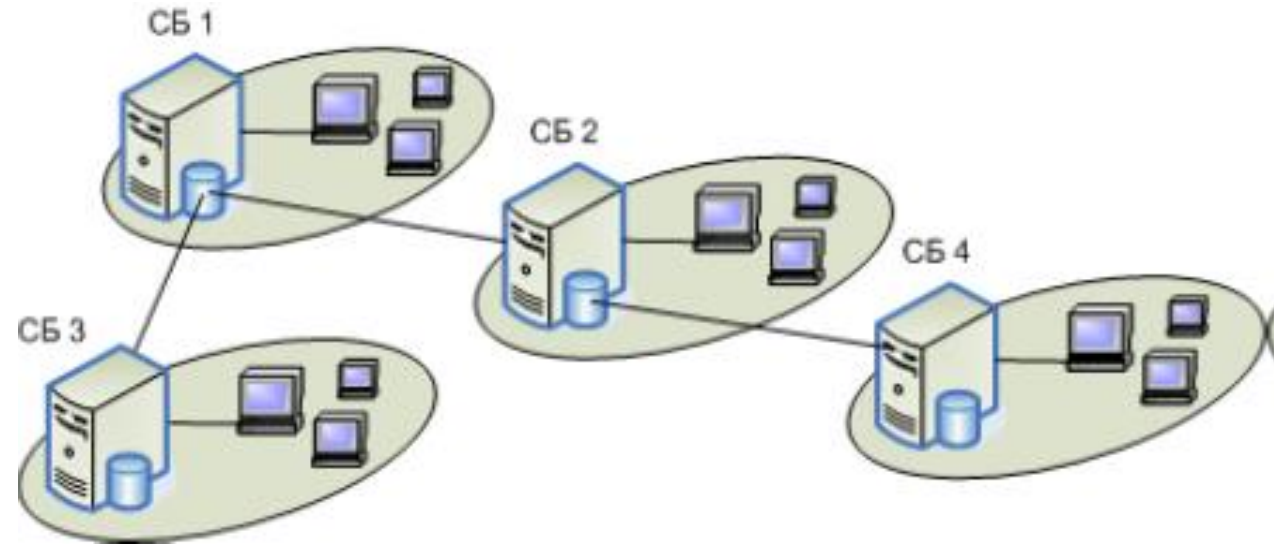
Автономный режим



Сетевой режим

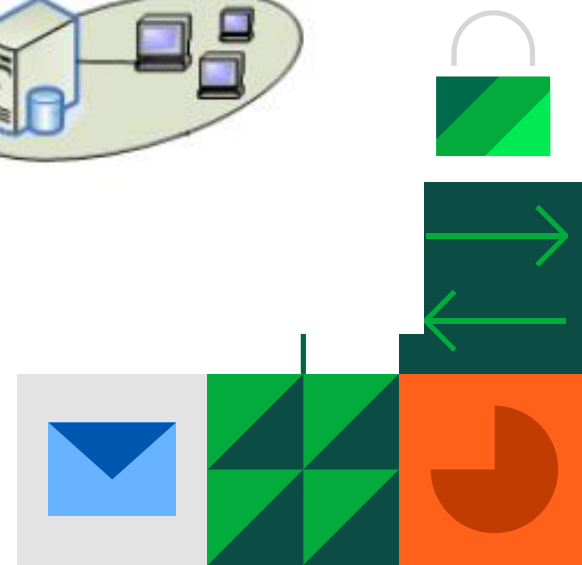


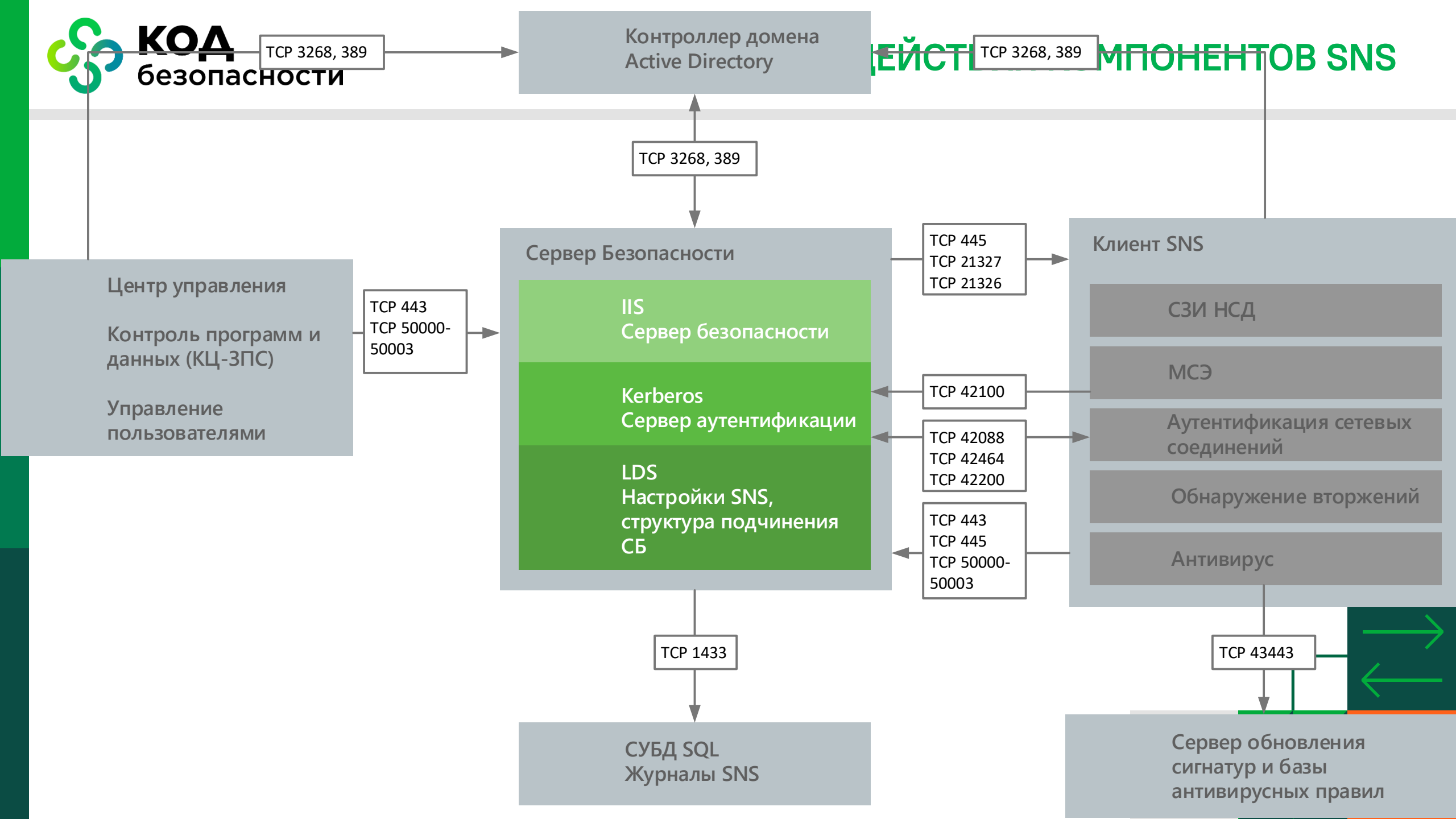
- **Домен безопасности** — это совокупность компьютеров, пользователей, серверов безопасности и их настроек, логически составляющих контейнер AD.
- Несколько доменов безопасности (со своими серверами безопасности) могут образовывать **лес доменов**.





- Для взаимодействия лесов безопасности используется специальный **шлюз**, который размещается в каждом из дочерних лесов безопасности. Все они регистрируются на родительском сервере безопасности.
- Все леса безопасности, относящиеся к данному серверу, формируют единое объединение – **федерацию**.





| Протокол/порт              | Назначение                                                                                                                                | Источник/получатель                                                        |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| <b>TCP / 443</b>           | IIS, соединение ПУ с сервером безопасности, соединение клиента SNS с СБ, передача команд управления, передача журналов, получение политик | Программа управления / СБ<br>Клиент SNS / СБ                               |
| <b>TCP / 3268 (389)</b>    | Обращение к AD: считывание из АД значений параметров и запись в АД изменений                                                              | Программа управления / контроллер домена<br>Клиент SNS / контроллер домена |
| <b>TCP / 50000 – 50003</b> | Обращение к AD LDS: считывание из AD LDS значений параметров и запись в AD LDS изменений                                                  | СБ / AD LDS<br>Программа управления / AD LDS<br>Клиент SNS / AD LDS        |
| <b>TCP / 21326</b>         | Служба подсистемы аппаратной поддержки                                                                                                    | Клиент SNS / СБ                                                            |
| <b>TCP / 21327</b>         | Служба подсистемы КЦ                                                                                                                      | Программа КЦ-ЗПС / клиент SNS                                              |
| <b>TCP / 1433</b>          | SQL-сервер – хранение журналов                                                                                                            | СБ / SQL-сервер                                                            |

**Табл.33 Открытые порты для всех компьютеров и серверов (общесистемные разрешения для работы с AD)**

| Назначение                    | TCP         | UDP               |
|-------------------------------|-------------|-------------------|
| Взаимодействие с AD           | 49152-65535 | 49152-65535       |
| Взаимодействие с DNS-сервером | 49152-65535 | 53<br>49152-65535 |
| NetBIOS name resolution       | -           | 137               |
| NetBIOS datagram service      | -           | 138               |
| NTP-синхронизация времени     | -           | 123               |

**Табл.34 Открытые порты для контроллера домена**

| Назначение                                     | TCP  | UDP |
|------------------------------------------------|------|-----|
| Доступ к LDAP                                  | 389  | 389 |
| Доступ к LDAPS                                 | 636  | -   |
| Механизм GPO, другие взаимодействия с AD       | 445  | -   |
| Служба сеанса NetBIOS                          | 139  | -   |
| Kerberos аутентификация пользователя           | 88   | -   |
| RPC-взаимодействия                             | 135  | -   |
| Доступ к Global Catalog                        | 3268 | -   |
| Доступ к Global Catalog по SSL (если настроен) | 3269 | -   |

**Табл.35 Открытые порты для других серверов**

| Назначение | TCP  | UDP  |
|------------|------|------|
| DNS-сервер | 53   | 53   |
| SQL-сервер | 1433 | 1434 |

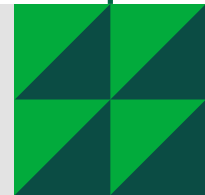
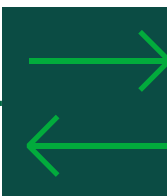


**Табл.36 Открытые порты для сетевого оборудования**

| Назначение                  | TCP   | UDP        |
|-----------------------------|-------|------------|
| Network broadcast           | -     | 137<br>138 |
| Обновление антивируса и COB | 43444 | 43444      |

**Табл.37 Открытые порты для работы всех СБ Secret Net Studio**

| Назначение                                  | TCP    | UDP   |
|---------------------------------------------|--------|-------|
| Интерфейс управления сервера аутентификации | 42100  | -     |
| Центр распространения ключей Kerberos       | 42088  | 42088 |
| Смена пароля пользователя Kerberos          | 42464  | 42464 |
| Взаимодействие с Центром управления         | 443    | -     |
| Взаимодействие с Secret Net LDS             | 50000* | -     |
| Взаимодействие с Secret Net LDS по SSL      | 50001* | -     |
| Взаимодействие с Secret Net-GC LDS          | 50002* | -     |
| Взаимодействие с Secret Net-GC LDS по SSL   | 50003* | -     |

**Табл.38 Открытые порты для работы родительского и подчиненного СБ Secret Net Studio**

| Назначение                      | TCP | UDP |
|---------------------------------|-----|-----|
| RPC-взаимодействия              | 135 | -   |
| Взаимодействие между СБ по HTTP | 443 | -   |

**Табл.39 Открытые порты для работы СБ, которому подчинен клиент Secret Net Studio**

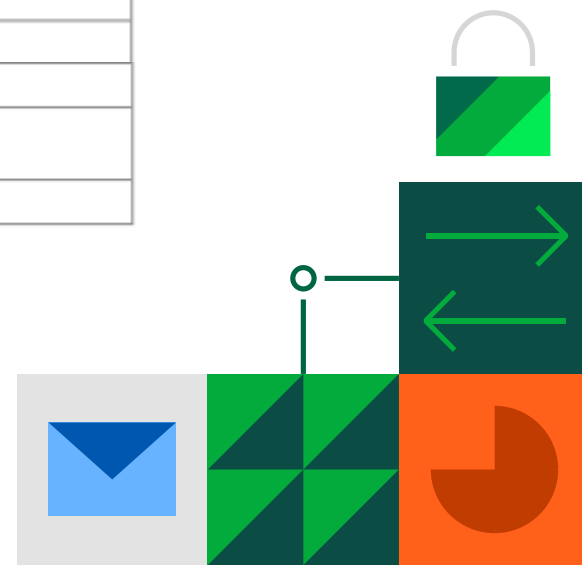
| Назначение                          | TCP | UDP |
|-------------------------------------|-----|-----|
| RPC-взаимодействия                  | 135 | -   |
| Взаимодействие СБ и клиента по HTTP | 443 | -   |
| Автоматическая установка клиента    | 139 | 137 |

**Табл.40 Открытые порты для работы сервера обновлений Secret Net Studio**

| Назначение                  | TCP   | UDP   |
|-----------------------------|-------|-------|
| Обновление антивируса и COB | 43444 | 43444 |

**Табл.41 Открытые порты для работы клиента Secret Net Studio**

| Назначение                                                                      | TCP   | UDP   |
|---------------------------------------------------------------------------------|-------|-------|
| Автоматическая установка клиента с СБ                                           | 445   | 137   |
| RPC-взаимодействие с СБ при централизованной установке клиента                  | 135   | -     |
| Аппаратная поддержка                                                            | 21326 | -     |
| Синхронизация настроек механизмов КЦ, ЗПС                                       | 21327 | -     |
| Согласование ключей ipsec, протокол ISAKMP согласования параметров безопасности | -     | 42200 |
| Обновление антивируса и COB                                                     | 43444 | 43444 |



# ОБЩИЙ ПОРЯДОК УСТАНОВКИ

1

- Подготовить организационные подразделения и включить в них нужные компьютеры для формирования доменов безопасности

2

- Для каждого леса доменов безопасности создать группу пользователей – администраторов леса

3

- Создать группы пользователей – администраторов доменов безопасности

4

- На компьютере корневого СБ: группы администраторов леса и домена безопасности включить в группу локальных администраторов

5

- На компьютере корневого СБ установить ПО сервера безопасности и клиента

6

- Выполнить действия 4 и 5 на всех подчиненных серверах безопасности

7

- На рабочих местах администраторов Secret Net Studio установить программу управления

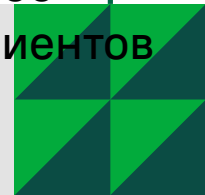
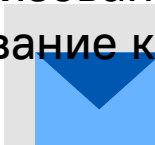
8

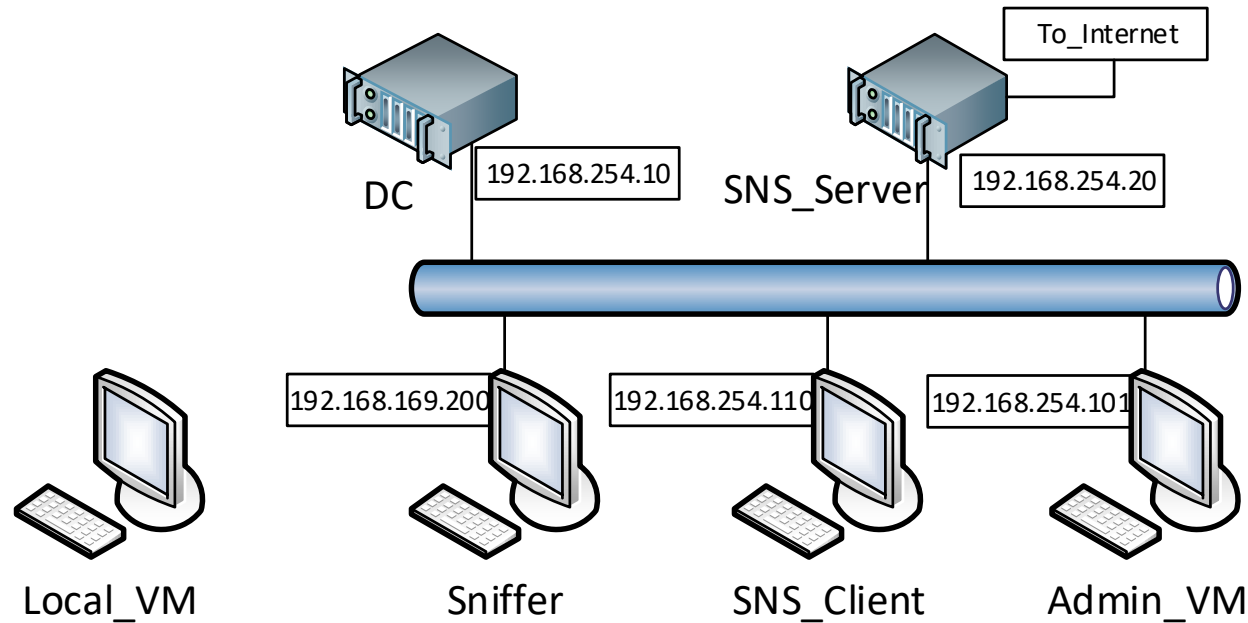
- Установить ПО клиента системы SNS на клиентских компьютерах

Подготовка структуры  
оперативного управления

Установка серверов  
безопасности

Установка Центров управления  
и централизованное  
развертывание клиентов

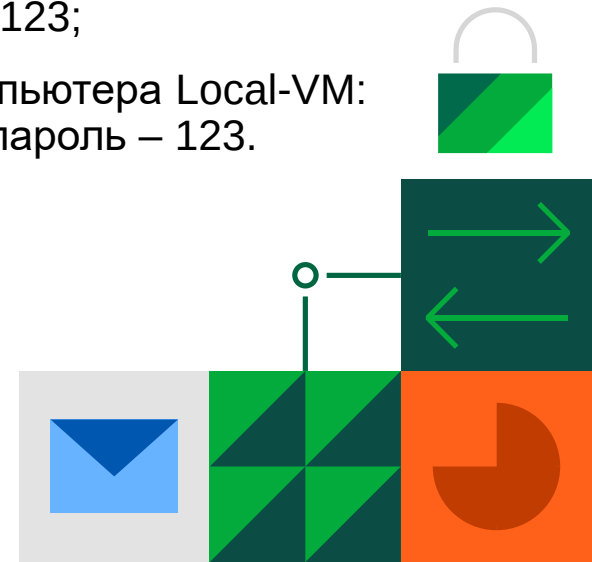




## Учетные записи:

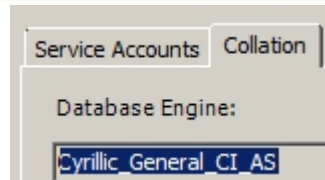
- администратор домена: "Администратор", пароль – 123 ;
- администратор домена безопасности: "snsadmin", пароль – 123;
- пользователи домена: "user1" и "user2", пароль 123 ;
- администратор компьютера Local-VM: "admin", пароль – 123;
- пользователи компьютера Local-VM: "user1" и "user2", пароль – 123.

Описание стенда – в файле "sns\_stand.doc"

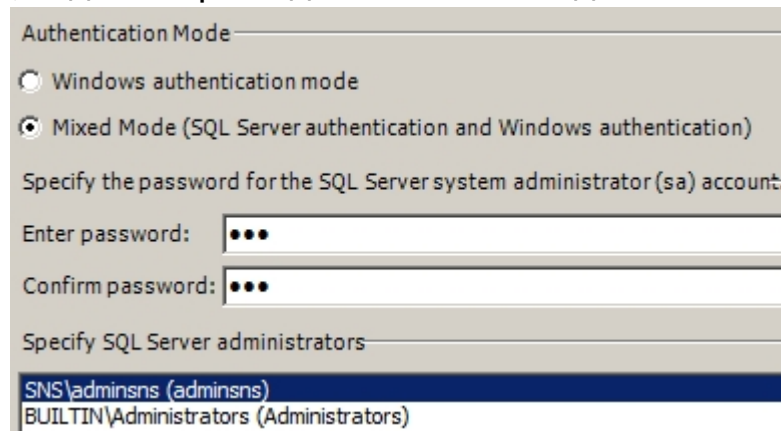


1. Проверить наличие нужных учётных записей пользователей и групп в AD
2. Проверить, что на будущем СБ группы администраторов Домена Безопасности – внесены в группу локальных администраторов.
3. На будущем СБ проверить, что включён компонент Microsoft .NET Framework 3.5
4. Проверить, что установлен Microsoft .NET Framework .NET 4.5 или выше
5. Установить Microsoft SQL 2012 или выше (с соблюдением требований)
6. Для MS SQL включить TCP и задать порт
7. Установить СБ с соблюдением требований
8. Установить ЦУ на ARM2
9. Использовать ЦУ для загрузки SNS в репозиторий, указать лицензию
10. Использовать ЦУ для развёртывания клиента SNS на СБ
11. Перезагрузить СБ по окончании установки клиента
12. Вновь в ЦУ подключиться к СБ и произвести удалённую установку клиента  
на ARM1 (все защитные механизмы включены)  
на ARM2 (все защитные механизмы выключены)

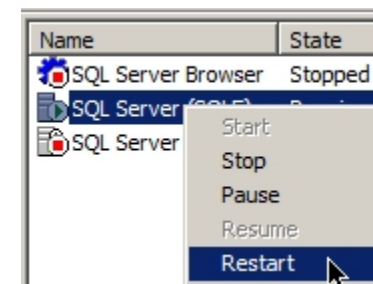
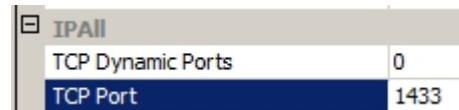
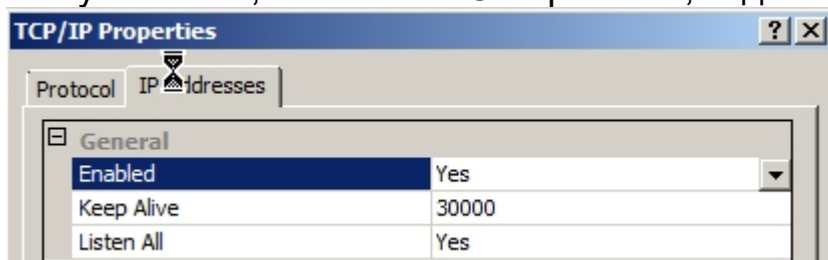
1) Проверить кодировку страницы поиска (Cyrillic)



2) Включить смешанный режим аутентификации, задать пароль для sa записи и добавить в администраторы локальных администраторов



3) После установки, включить TCP протокол, задать порт 1433 и перезапустить сервис SQL.



1) на этапе выбора охвата Домена Безопасности, оставить OU (выбран автоматически), а также в качестве имени домена ввести указанное.

Выберите контейнер Active Directory (домен или организационное подразделение), с которым будет связан домен безопасности. Объекты контейнера будут включены в состав домена безопасности.

sns.local/ou\_sns

Введите имя домена безопасности:

SNS.LOCAL.OU-SNS

Пример: SNS.LOCAL.OUFSNS

2) выбрать нужные группы админов домена безопасности и леса доменов

Группа пользователей, которой будут предоставлены права администрирования домена безопасности.

SNS\snsadmin

Изменить...

Группа пользователей, которой будут предоставлены права администрирования леса доменов безопасности.

SNS\snsadmin\_forest

Изменить...

3) На этапе выбора SQL вписать «имя\_сервера\имя\_SQL», учётной записью администратора БД задать sa (или любого другого админа SQL) в качестве учётной записи, используемой для доступа к БД – указать нового пользователя (он будет создан автоматически).

Имя БД: server\sqli

Учетная запись администратора БД

Имя: sa

Пароль: ...

Учетная запись, используемая сервером для доступа к БД

Имя: sqluser

Пароль: ...

4) Перезагрузить сервер по окончании установки.

Виртуальные машины представлены для применения в VMware.

Лабораторные находятся в папке  
sns\Course\L\

L0.pdf – как добавлять и предварительно настраивать ВМ.

L0a.pdf – как добавить нужные группы домена в локалмин. с помощью ГП

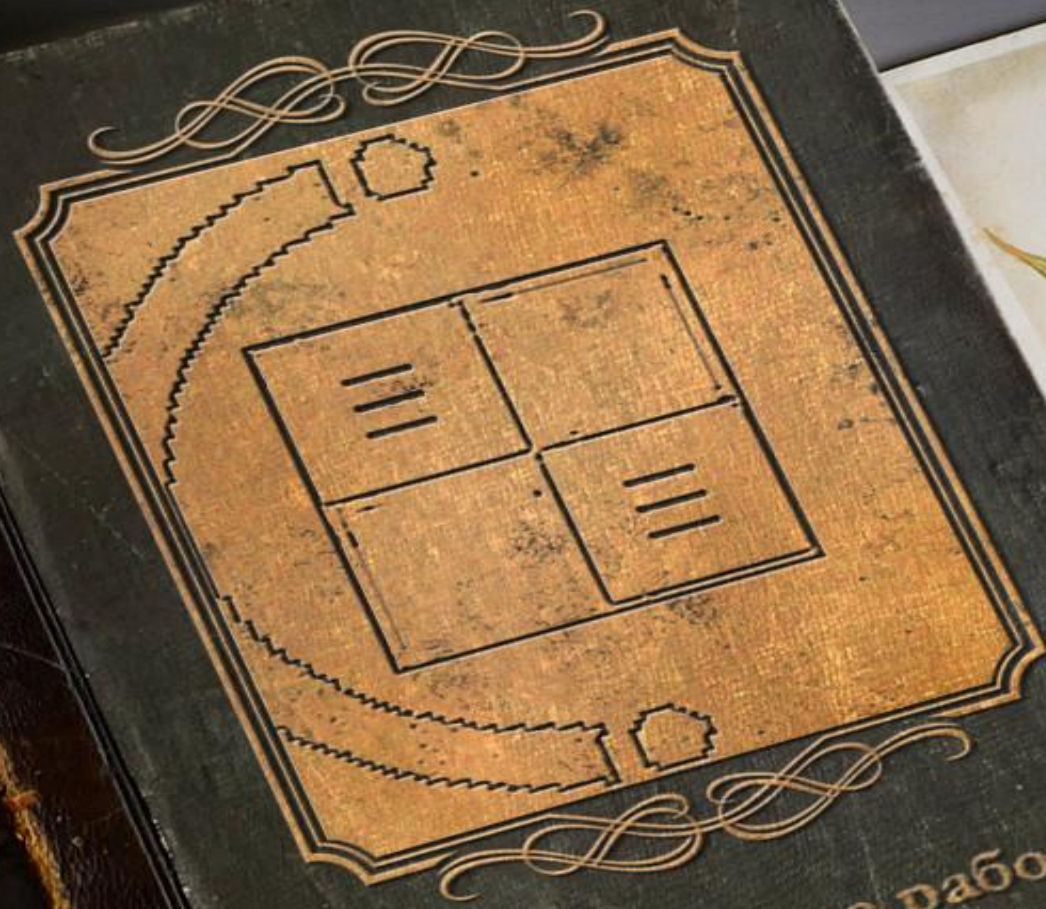
Первый день практики  
L0.pdf, L0a.pdf, L1.pdf

В папках Alt, Alt-2021, Alt1 представлены множество дополнительных материалов, не включённых в курс.

Второй день практики  
L2.pdf

В файле sns\txt\urls.txt представлены полезные ссылки:  
на видео по продукту, на страницу продукта, а также  
на страницу, где скачать стенд от Код Безопасности.

Третий день практики  
L3.pdf, L5.pdf, L6.pdf, L7.pdf



Лабораторные работы  
Код Безопасности





**КОД**  
безопасности



**СПАСИБО ЗА ВНИМАНИЕ!**



АКАДЕМИЯ  
ИНФОРМАЦИОННЫХ  
СИСТЕМ

## Лабораторный модуль 1

ООО «Код Безопасности»  
[www.securitycode.ru](http://www.securitycode.ru)  
[education@securitycode.ru](mailto:education@securitycode.ru)

Академия Информационных Систем  
[www.infosystem.ru](http://www.infosystem.ru)  
[security@infosystem.ru](mailto:security@infosystem.ru)

