



SECUROS v5.2

Руководство по установке

Версия 5.2

Руководство по установке SecurOS (IG-Ru, сборка 15 от 16 февраля 2010 г.).

© Copyright ISS Technology 2005–2010

Отпечатано в России.

ISS Technology оставляет за собой право вносить изменения как в данное Руководство, так и в описываемый продукт. Изменения могут вноситься в спецификацию системы без уведомления. Содержимое Руководства не является офертой, гарантией, обещанием или условием договора, и не должно восприниматься подобным образом.

Никакая часть данной документации не может быть воспроизведена, передана, процитирована, размещена в поисковой системе, переведена на любой язык или машинный код в любой форме и любыми средствами без явного письменного согласия со стороны правообладателя. Несанкционированное копирование этой публикации может не только нарушить авторские права, но и ослабить возможность ISS Technology предоставлять точную и актуальную информацию пользователям продукта.

Оглавление

Оглавление	3	2.1.3.1	Требования к серверу приложений	17
Предисловие	6	2.1.3.2	Требования к рабочему месту администратора	17
Назначение	6	2.1.3.3	Требования к рабочему месту оператора	18
Целевая аудитория	6	2.1.3.4	Требования к видеосерверу (видеоконцентратору)	18
Использование руководства	6	2.1.3.5	Требования к аудиоподсистеме	19
Обращение за технической поддержкой	6	2.1.3.6	Требования к подсистеме оповещения	19
1 Архитектура SecurOS	8	2.1.3.7	Требования подсистем контроля доступа и охранно-пожарной	19
1.1 Общие положения	8	2.2	Установка аппаратного обеспечения	19
1.2 Распределенное сетевое окружение	9	2.2.1	Установка ключа Guardant	19
1.3 Виды серверов и рабочих мест	9	2.2.2	Видеоподсистема	20
1.3.1 Сервер приложений	10	2.2.2.1	Установка видеоплаты	20
1.3.2 Видеосервер	10	2.2.2.2	Подключение видеокамер	21
1.3.3 Рабочее место оператора	10	2.2.2.3	Подключение видео-HUB и IP-камер	22
1.3.4 Рабочее место администратора	10	2.2.2.4	Подключение поворотных устройств (купольные камеры)	22
1.4 Модульная структура	11	2.2.3	Аудиоподсистема	24
2 Установка системы	12			
2.1 Общие сведения	12			
2.1.1 Последовательность процедуры установки	12			
2.1.2 Планирование системы	12			
2.1.2.1 Автономная конфигурация	13			
2.1.2.2 Централизованное видеонаблюдение	14			
2.1.2.3 Просмотр видео из удаленной сети	14			
2.1.3 Проверка требований системы	16			

Оглавление

2.2.4	Подсистема оповещения . .	24	П2.2.2	Каскадное подключение плат TVISSx-02	56
2.2.5	Охранно-пожарная подсистема и подсистема контроля доступа	24	П2.2.3	Подключение аудиовходов	57
2.2.6	Соединение компьютеров в единую сеть	24	П2.2.4	Подключение схемы Watchdog	57
2.3	Установка программного обеспечения	25	П2.2.5	Подключение платы расширения TVISS8IO к плате TVISS1-02	58
2.3.1	Содержимое компакт-диска	25	П2.3	Описание платы TVISS4-02EXT . . .	59
2.3.2	Процедура установки . . .	26	П2.3.1	Подключение платы TVISS4-02	59
2.4	Обновление программного обеспечения	35	П2.3.2	Подключение аудиовходов	59
2.5	Удаление программного обеспечения	35	П2.4	Описание плат TVISS4E и TVISS8E .	59
3	Запуск системы	36	П2.4.1	Подключение видеокамер .	60
3.1	Запуск на сервере / рабочем месте администратора	36	П2.4.2	Подключение аудиовходов	60
3.1.1	Первый запуск	37	П2.4.3	Каскадное подключение плат TVISSxE	62
3.2	Открытие и закрытие панели управления	47	П2.4.4	Подключение схемы Watchdog	62
3.3	Выход из системы	48	П2.4.5	Подключение платы расширения TVISS8IO к плате TVISS4E (TVISS8E) . .	63
Приложение 1.	Часто задаваемые вопросы	49	П2.5	Описание плат TVISS PCI-E8 R1 и TVISS A8 R1	63
Приложение 2.	Платы видеозахвата	52	П2.5.1	Подключение видеокамер .	64
П2.1	Описание платы TVISS4-02	52	П2.5.2	Подключение аудиовходов	65
П2.1.1	Подключение платы расширения TVISS4-02EXT . . .	52	П2.5.3	Подключение схемы Watchdog	65
П2.1.2	Подключение видеокамер .	52	П2.5.4	Подключение платы расширения TVISS A8 R1 к плате TVISS PCI-E8 R1 .	65
П2.1.3	Каскадное подключение плат TVISSx-02	53	П2.5.5	Подключение платы расширения TVISS8IO к плате TVISS PCI-E8 R1	66
П2.1.4	Подключение аудиовходов	53	П2.5.6	Индикация состояния . . .	66
П2.1.5	Подключение схемы Watchdog	54	П2.6	Описание платы TVISS8IO	67
П2.1.6	Подключение платы расширения TVISS8IO к плате TVISS4-02	55	П2.6.1	Подключение питания . . .	67
П2.2	Описание платы TVISS1-02	56			
П2.2.1	Подключение видеокамер .	56			

Оглавление

П2.6.2 Подключение платы TVISS8IO к TVISSx-02 и TVISSxE	68	П5.2 Подключение купольных камер к видеосерверу Bosch VIP X1	81
П2.6.3 Каскадное подключение плат TVISS8IO	68	П5.3 Подключение купольных камер к видеосерверам AXIS	82
П2.6.4 Настройка цифровых входов и выходов	68	П5.4 Особенности подключения некоторых видеокамер и HUB-устройств	84
Приложение 3. Технические данные	72	Приложение 6. Совместимость аппаратного обеспечения	85
П3.1 Разрешение изображения	72	П6.1 Системные платы	85
П3.2 Рекомендуемые процессоры для видеосерверов	72	П6.2 Поворотные устройства	87
П3.3 Скорость передачи данных	73	П6.3 Модемы с поддержкой голосовых сообщений	89
П3.4 Размер видеокadra	74	Приложение 7. Системные утилиты	90
П3.5 Время хранения видеоархива / объем жесткого диска	75	П7.1 Утилита ISS Hardware Report	90
Приложение 4. Используемые в SecurOS порты	77	П7.2 Утилита ISS System Report	91
Приложение 5. Установка аппаратного обеспечения сторонних производителей	80	П7.3 Утилита ISS Startup Configuration	93
П5.1 Подключение купольной камеры Panasonic WV-CS850	80	П7.4 Утилита DSAdmin	94
		Глоссарий	96
		Предметный указатель	98



Предисловие

Назначение

В данном руководстве описывается архитектура SecurOS, процессы установки, обновления, удаления и запуска аппаратного и программного обеспечения SecurOS на сервере и клиентских компьютерах, содержатся советы и рекомендации по настройке для большей производительности операционной системы.

Целевая аудитория

Руководство предназначено для системных инсталляторов, интеграторов и администраторов — опытных пользователей операционной системы Microsoft® Windows®, имеющих навыки по установке аппаратного обеспечения и построению сети на основе протокола TCP/IP и знающих основы технологий CCTV.

Использование руководства

Данный документ можно использовать как в печатном, так и в электронном виде. В последнем случае доступны такие возможности ПО Adobe Reader, как закладки и гипертекстовые ссылки для навигации по документу. Данное руководство ссылается на другие документы по SecurOS ([Руководство администратора SecurOS](#), [Руководство пользователя SecurOS](#) и т. д.), которые можно найти на установочном диске SecurOS или на веб-сайте компании ISS (www.iss.ru).

Обращение за технической поддержкой

При наличии вопросов, ответы на которые отсутствуют в данном руководстве, обратитесь к своему системному интегратору.

За дальнейшей информацией обращайтесь в Службу технической поддержки компании ISS:

- по телефону:

+7 (495) 734 33 33 (многоканальный, с понедельника по четверг с 10:00 до 19:00,
в пятницу с 10:00 до 18:00 по московскому времени);

Предисловие

- по электронной почте:

support@iss.ru.

Примечание. Для более скорого разрешения проблем, рекомендуем подготовить служебную информацию, указанную в [Руководстве администратора SecurOS](#), перед обращением в Службу технической поддержки.

1. Архитектура SecurOS

SecurOS — интегрированная система безопасности, функционирующая в сети на базе протокола TCP/IP.

Подключение интеллектуальных модулей (например, модуля распознавания номеров автомобилей) и многих других дополнительных устройств обеспечивает возможность широкого использования сети безопасности.

1.1 Общие положения

- Неограниченное количество серверов и рабочих мест, подключенных к сети, работающей по протоколу TCP/IP.
- Поддержка использования различных IP-видеокамер, поворотных и аудиоустройств.
- Возможность создания различных по функциональности и производительности систем.
- Возможность неограниченного расширения системы дополнительным аппаратным и программным обеспечением.
- Возможность конфигурации всей охранной сети с любого сервера.
- Многофункциональный интерфейс пользователя.
- Возможность оповещения о тревожных ситуациях по электронной почте.
- Поддержка скриптов для реализации любой логики охранной системы.

1.2 Распределенное сетевое окружение

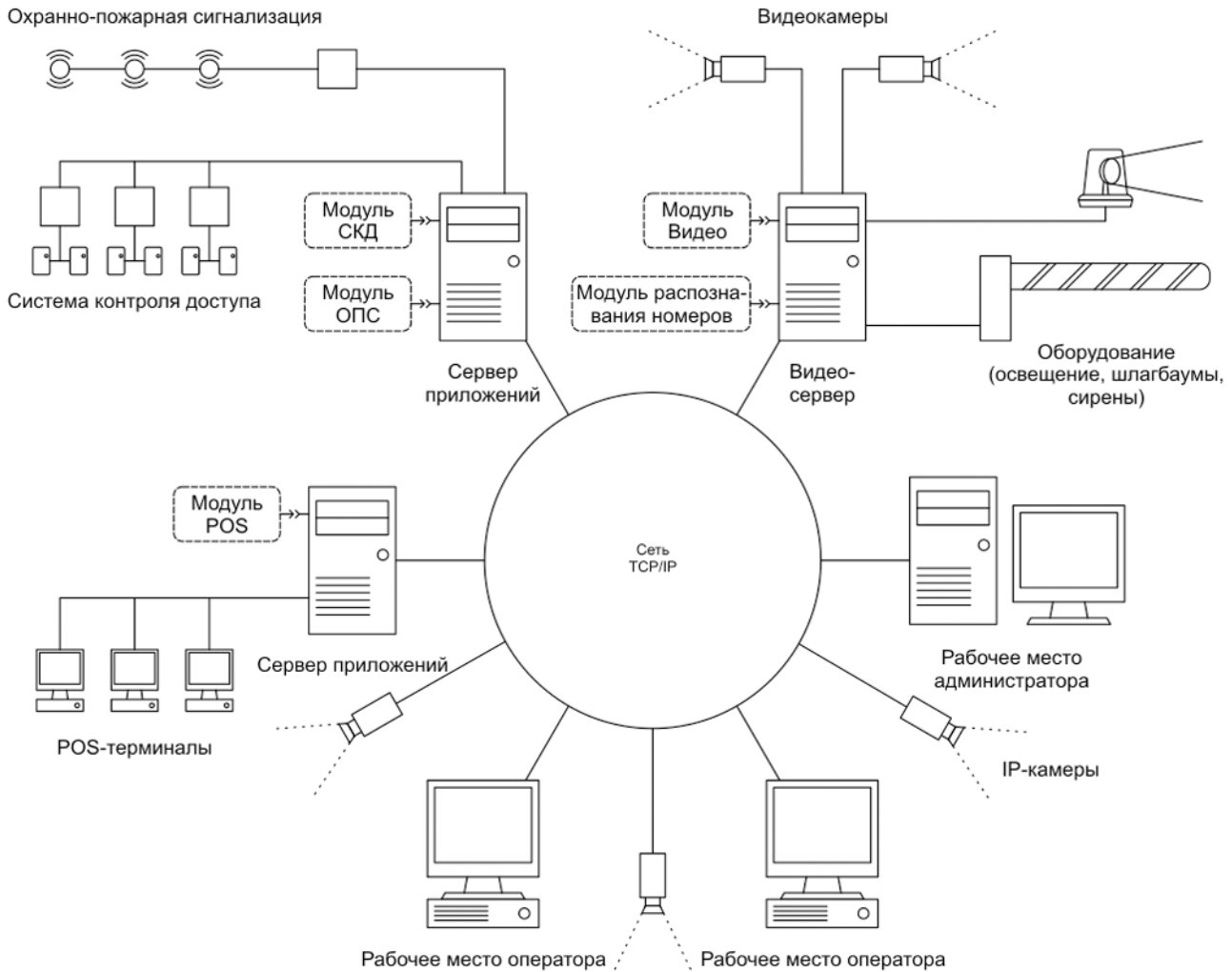


Рис. 1. Пример планирования архитектуры SecurOS

1.3 Виды серверов и рабочих мест

Все компьютеры, входящие в сеть SecurOS, делятся по своему функциональному назначению на три группы: сервер приложений, рабочее место администратора и рабочее место оператора. Отдельно выделяется *видеосервер* как сервер приложений с платой/платами видеозахвата.

1.3.1 Сервер приложений

Сервер приложений представляет собой компьютер, управляющий определенным сегментом охранной сети. Все охранные устройства (видеокамеры, платы видеозахвата, аудиоплаты, контроллеры охранно-пожарной тревоги, подсистема контроля доступа и т. д.) и интеллектуальные программные модули (например, модуль распознавания номеров автомобилей) должны быть подсоединены или установлены на серверы.

Каждый сервер при условии надлежащей настройки имеет права на администрирование сети безопасности, поэтому можно проводить конфигурацию всей сети SecurOS на таком сервере (при наличии монитора).

Чтобы использовать отдельный компьютер для удаленного администрирования, настройте его как рабочее место администратора (см. ниже) или используйте удаленное соединение Microsoft (протокол RDP) для удаленного доступа к любому серверу с любого компьютера, находящегося в домене сети.

1.3.2 Видеосервер

Видеосервер — это сервер приложений с одной или более платами видеозахвата, предназначенный для получения и обработки видеопотока с видеокамер и IP-камер.

1.3.3 Рабочее место оператора

Рабочее место оператора — это клиентский компьютер в сети безопасности, предназначенный для удаленного просмотра видео, получаемого с видеокамер или IP-камер, прослушивания звука, управления различными устройствами, например поворотными устройствами, дверями, охранно-пожарной и другими подсистемами.

1.3.4 Рабочее место администратора

Рабочее место администратора — это клиентский компьютер, аналогичный рабочему месту оператора, но обладающий дополнительным интерфейсом администратора для конфигурации сети безопасности. На таком компьютере можно проводить следующие операции:

- Создавать и конфигурировать объекты системы.
- Удалять существующие объекты.
- Изменять параметры созданных и работающих объектов.

1.4 Модульная структура

Модульная структура обеспечивает следующие возможности:

- подключение специализированных модулей (например, модуль распознавания номеров автомобилей, модули для подключения дополнительных сигнальных устройств или устройств контроля доступа) к существующей сети SecurOS для расширения функциональности сети;
- автоматическое определение загружаемых модулей и подсистем (в зависимости от конфигурации системы) программным обеспечением каждого сервера приложений для обеспечения высокой производительности.

2. Установка системы

2.1 Общие сведения

2.1.1 Последовательность процедуры установки

1. Планирование системы: сколько серверов и рабочих мест необходимо, какое аппаратное и дополнительное программное обеспечение следует установить.
2. Проверка требований системы к каждому серверу и рабочему месту охранной сети: требования каждой подсистемы (видеоконтроль, аудиоконтроль, контроль доступа и т. д.) зависят от ее функциональности.
3. Установка необходимого аппаратного обеспечения (видеоплаты, ключа Guardant и т. д.) на каждом сервере и подключение внешних устройства (контроллеры, камеры, микрофоны и т. д.).
4. Объединение всех серверов и рабочих мест в единую сеть.
5. Установка программного обеспечения SecurOS на каждом клиентском компьютере/сервере.

2.1.2 Планирование системы

Рационально спланируйте свою систему безопасности перед тем, как приобрести ее. Максимальное количество серверов приложения, видеосерверов, рабочих мест оператора и администратора, как и количество подключаемых модулей на каждый сервер и в сеть SecurOS в целом, определяется файлом лицензионного ключа. Для оптимизации своей сети безопасности SecurOS обратитесь к своему системному интегратору.

Перед началом установки системы определите необходимое количество серверов приложений, видеосерверов, рабочих мест оператора и администратора:

- Количество видеосерверов зависит от количества устанавливаемых камер. Их количество определяет скорость передачи кадров — количество кадров в секунду (к/с). Например, при наличии 16 камер, работающих со скоростью 12 к/с, общая скорость передачи составит $16 \times 12 = 192$ к/с. Передовые серверы могут поддерживать скорость до 400 к/с. Для сервера можно использовать скорость 200 к/с. Например, при сорока камерах, со скоростью передачи 25 к/с каждая, общая скорость составит 800. Таким образом, потребуется четыре видеосервера (или два передовых видеосервера). Более подробную информацию о видеосерверах см. в разделе [Приложение 3. Технические данные](#) на стр. 72.
- Количество серверов приложений (исключая видеосерверы) определяет, какими устройствами (не видео-) ваша сеть SecurOS будет управлять. Если загрузка видеосерверов небольшая, то есть процессор загружен менее чем на 50%, то возможна установка дополнительных модулей, например модуля распознавания номеров автомобилей, модуля контроля доступа. Общая

загрузка процессора не должна превышать 75%. В противном случае следует передать эти функции другому серверу приложений для сохранения баланса загрузки. Один сервер приложений может одновременно работать с системой контроля доступа и охранно-пожарной сигнализацией; однако интеллектуальные модули распознавания (например, модуль распознавания номеров автомобилей) следует запускать на разных серверах. Дополнительные серверы (видеоконцентраторы) также могут быть использованы для уменьшения загрузки сети или удаленного просмотра видео (см. раздел [2.1.2.3 Просмотр видео из удаленной сети](#) на стр. 14).

- Количество рабочих мест оператора зависит от количества операторов, которые будут работать с системой. Необходимо учитывать, что назначение большого количества ресурсов оператору значительно снижает его производительность. Рекомендуется устанавливать 8 камер на одно рабочее место (в этом случае на каждого оператора будет приходиться по 8 камер). Кроме того, необходимы отдельные рабочие места для системы контроля доступа и охранно-пожарного мониторинга, модуля распознавания номеров автомобилей и т. д.
- Для некоторых конфигураций может понадобиться рабочее место администратора. Это необходимо, если и серверы приложений, и видеосерверы не оборудованы мониторами либо если загрузка всех серверов максимальна. В противном случае можно использовать любой сервер приложений или видеосервер для администрирования сети.

2.1.2.1 Автономная конфигурация

Такая конфигурация подходит для относительно небольших систем. В данном случае сервер представляет собой и рабочее место оператора, и рабочее место администратора (см. рис. 2). Сервер может быть не подсоединен к сети (автономный режим).

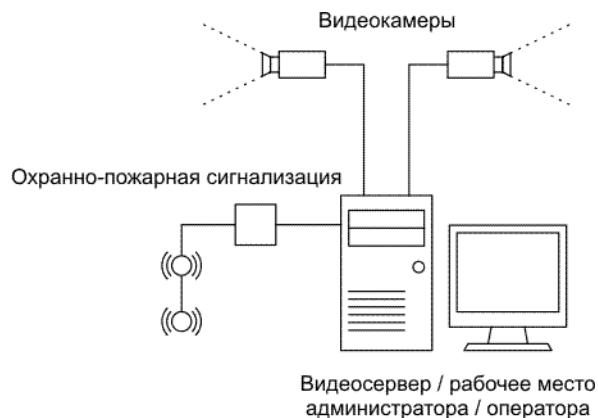


Рис. 2. Схема автономной установки SecurOS

2.1.2.2 Централизованное видеонаблюдение

Такая конфигурация подходит для центров видеонаблюдения в многолюдных местах, например для аэропортов, железнодорожных станций, казино (см. рис. 3).

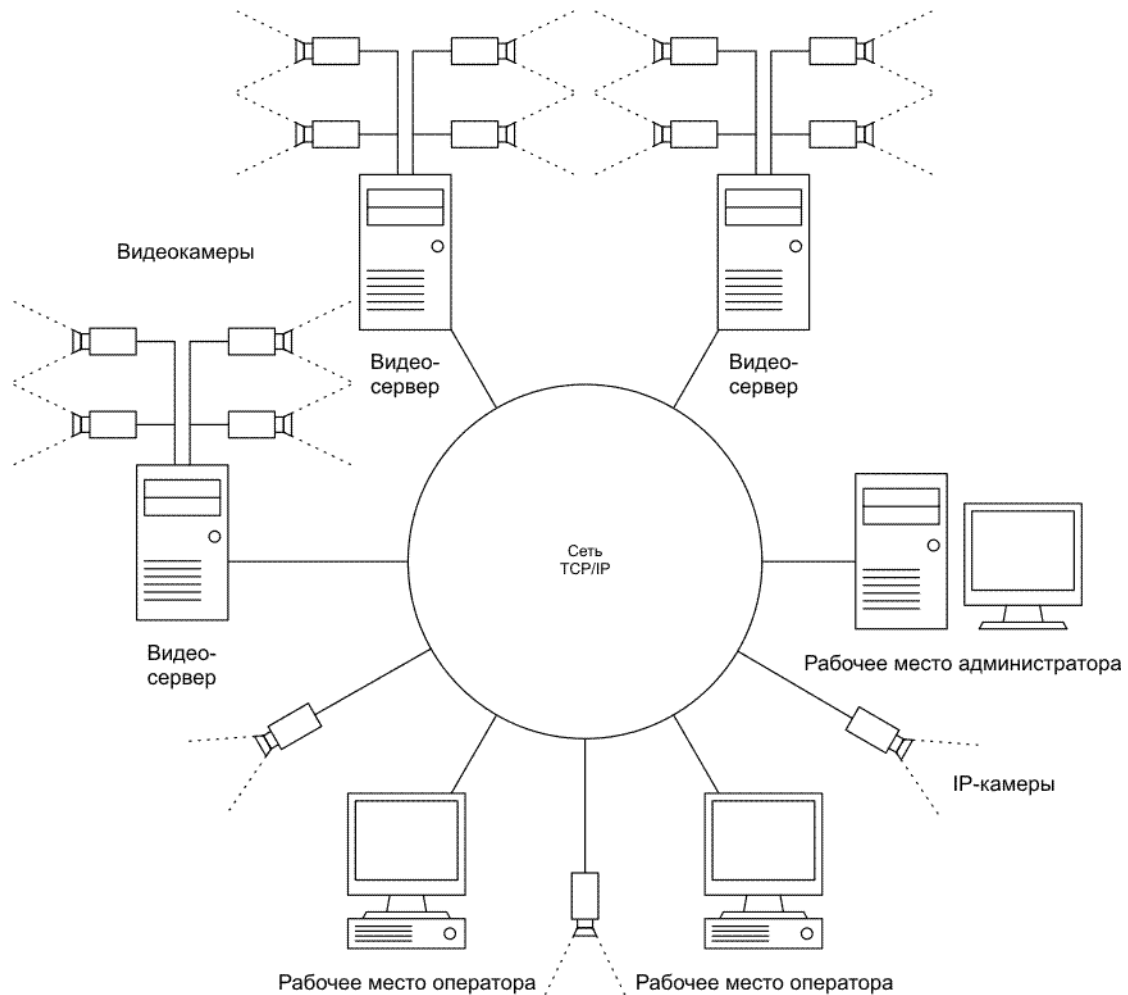


Рис. 3. Схема централизованного видеонаблюдения

2.1.2.3 Просмотр видео из удаленной сети

Если компоненты системы находятся в разных локальных сетях, соединенных по низкоскоростным каналам связи, и требуется удаленный просмотр видео, то необходимо использовать видеоконцентратор. Видеоконцентратор является сервером приложений, который получает видеопоток из удаленной сети и передает его рабочим местам оператора, находящимся в их локальной сети (см. рис. 4).

Установка системы

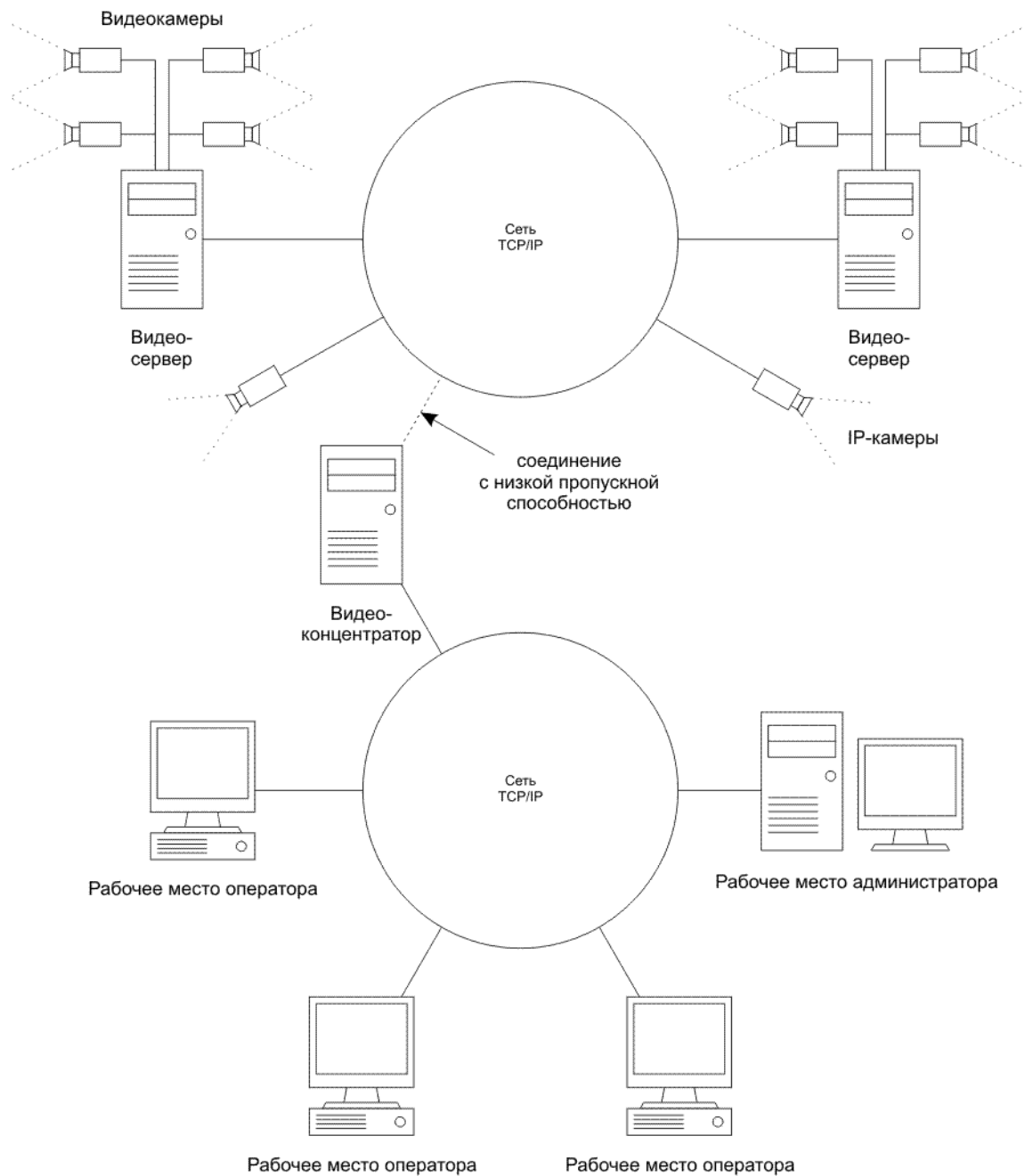


Рис. 4. Просмотр видео из удаленной сети

На рис. 5 приведена схема подключения рабочих мест оператора с каждым видеосервером и приема с них копий видеопотока; на рис. 6 — схема соединения через видеоконцентратор, когда он получает видеопоток от видеосерверов и передает его рабочим местам оператора, уменьшая нагрузку видеосервера и сети.

Установка системы

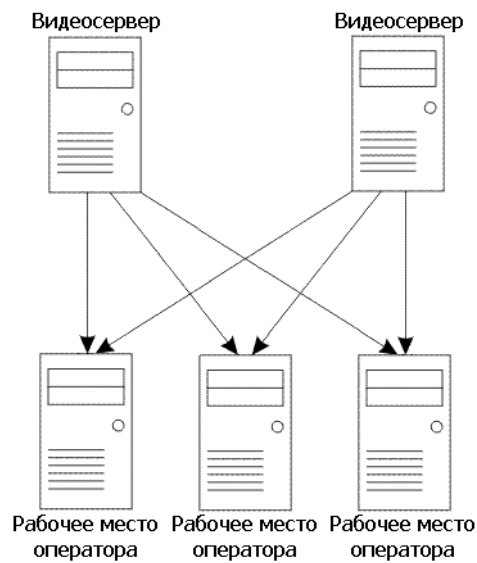


Рис. 5. Схема передачи данных в сети SecurOS без видеоконцентратора

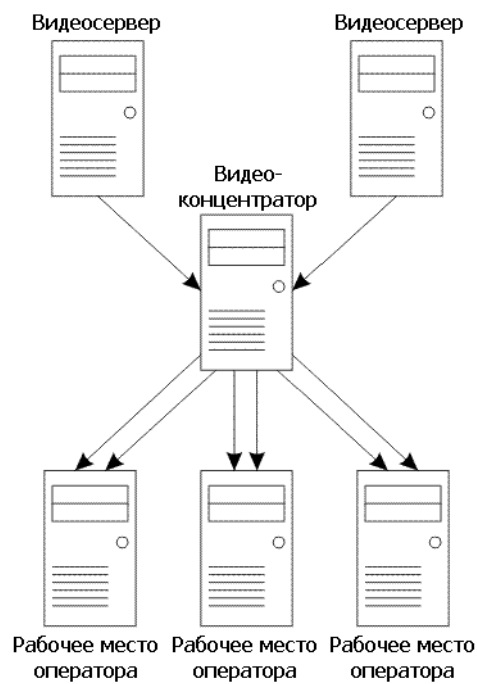


Рис. 6. Схема передачи данных в сети SecurOS с видеоконцентратором

2.1.3 Проверка требований системы

Перед установкой аппаратного и программного обеспечения SecurOS ознакомьтесь с приведенными ниже требованиями системы и убедитесь, что оборудование им полностью удовлетворяет.

2.1.3.1 Требования к серверу приложений

Таблица 1. Системные требования к серверу приложений

Параметр	Требования
Операционная система	Windows 2000 (Service Pack 4), Windows XP (Service Pack 2) или Windows Server 2003 (Service Pack 1)
Системная плата	См. раздел П6.1 Системные платы на стр. 85
Процессор	Intel Celeron 2 ГГц или более производительный
Оперативная память	Не менее 512 МБ
Размер жесткого диска	Не менее 40 ГБ
Пропускная способность канала связи по протоколу TCP/IP	Не менее 10 Мбит/с (в случае соединения клиент-сервер)

2.1.3.2 Требования к рабочему месту администратора

Таблица 2. Системные требования к рабочему месту администратора

Параметр	Требования
Операционная система	Windows 2000 (Service Pack 4), Windows XP (Service Pack 2)
Системная плата	См. раздел П6.1 Системные платы на стр. 85
Процессор	Intel Celeron 400 МГц или более производительный
Оперативная память	Не менее 128 МБ
Размер жесткого диска	Не менее 40 ГБ
Пропускная способность канала связи по протоколу TCP/IP	Не менее 10 Мбит/с

2.1.3.3 Требования к рабочему месту оператора

Таблица 3. Системные требования к рабочему месту оператора

Параметр	Требования
Операционная система	Windows 2000 (Service Pack 4), Windows XP (Service Pack 2)
Системная плата	См. раздел П6.1 Системные платы на стр. 85
Процессор	Intel Celeron 2 ГГц или более производительный (процессор должен поддерживать SSE2 в случае удаленного просмотра видео)
Оперативная память	Не менее 256 МБ
Размер жесткого диска	Не менее 40 ГБ
Видеоконтроллер	Любой SVGA-адаптер (кроме nVidia GeForce2) с 64 МБ памяти (предпочтительнее 128 МБ)
Пропускная способность канала связи по протоколу TCP/IP	Не менее 10 Мбит/с (или не менее 100 Мбит/с в случае удаленного просмотра видео)

2.1.3.4 Требования к видеосерверу (видеоконцентратору)

Таблица 4. Системные требования к видеосерверу (видеоконцентратору)

Параметр	Требования
Процессор	Pentium IV 2 ГГц или более производительный (процессор должен поддерживать SSE2)
Оперативная память	1 ГБ или более
Размер жесткого диска	150 ГБ или более
Видеоконтроллер	Любой SVGA-адаптер (кроме nVidia GeForce2) с 64 МБ памяти (предпочтительнее 128 МБ)
Пропускная способность канала связи по протоколу TCP/IP	Не менее 100 Мбит/с (в случае соединения клиент-сервер)

Примечание. Требования к видеосерверу (видеоконцентратору) зависят от поддерживаемого сервером общего значения скорости передачи кадров (для выбора процессора и жесткого диска см. раздел [Приложение 3. Технические данные](#) на стр. 72).

2.1.3.5 Требования к аудиоподсистеме

Сервер приложений должен иметь либо встроенную звуковую плату (см. руководство для системной платы), либо любую дополнительную звуковую PCI-плату. В качестве альтернативы можно использовать платы видеозахвата TVISS1-02, TVISS4-02, TVISS4E-REV5 или TVISS PCI-E8 R1, на которых имеется дополнительный аудиовход.

Примечание. Установка звуковой платы на сервер необходима, если с него будут прослушиваться аудиозаписи.

2.1.3.6 Требования к подсистеме оповещения

Чтобы использовать сервис голосовых сообщений (автоматические телефонные звонки с голосовым сообщением о событиях системы), следует подключить модем с поддержкой голосовых сообщений через последовательный порт (список модемов, совместимых с SecurOS, см. в разделе [П6.3 Модемы с поддержкой голосовых сообщений](#) на стр. 89).

Для использования сервиса звукового оповещения (звуковое сопровождение событий) на отдельном компьютере потребуется либо встроенная, либо дополнительная звуковая плата.

2.1.3.7 Требования подсистем контроля доступа и охранно-пожарной

Сервер приложений должен иметь определенное количество свободных последовательных портов в зависимости от подключаемых контроллеров подсистем (подсистема контроля доступа, охранно-пожарная сигнализация).

2.2 Установка аппаратного обеспечения

В данном разделе описывается процесс установки аппаратного обеспечения и даются рекомендации по установке дополнительного оборудования, таких как камеры, поворотные устройства, контроллеры (см. руководства по соответствующим устройствам и [Приложение 5. Установка аппаратного обеспечения сторонних производителей](#) на стр. 80).

2.2.1 Установка ключа Guardant

Ключ Guardant является электронным устройством, постоянно подключенным к компьютеру через USB-порт. Защищенное приложение обращается к ключу для проверки лицензионной информации.

Внимание! Ключ Guardant должен быть установлен на все компьютеры сети безопасности SecurOS, кроме серверов, которые оборудованы видеоплатами (работают на основе лицензионных ключей аппаратного обеспечения), и рабочих мест оператора.

Требуемое количество ключей Guardant выдается при приобретении системы SecurOS. Ключ необходимо установить перед началом установки программного обеспечения SecurOS.

Чтобы установить ключ Guardant, подсоедините ключ к свободному USB-порту компьютера.

2.2.2 Видеоподсистема

Установка видеосервера состоит из следующих этапов:

1. Установка одной или нескольких плат видеозахвата TVISS, приобретенных совместно с SecurOS.
2. Подключение видеокамер.
3. Подсоединение устройств видео-HUB и IP-камер к сети TCP/IP.
4. Подключение купольных камер к компьютеру или видео-HUB.

2.2.2.1 Установка видеоплаты

Внимание! Перед началом процесса установки отсоедините компьютер от электросети, чтобы обезопасить себя от поражения электрическим током, а компьютерное оборудование — от повреждения!

Откройте корпус системного блока для получения доступа к свободным PCI-слотам (см. рис. 7).

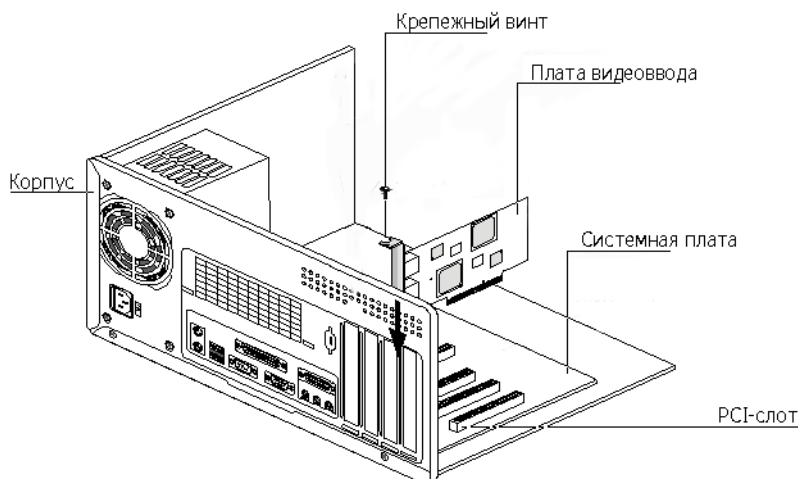


Рис. 7. Установка платы видеозахвата

Примечание. Не все платы видеозахвата совместимы с SecurOS (характеристики плат видеозахвата см. в разделе [Приложение 2. Платы видеозахвата](#) на стр. 52). На совместимых платах есть два основных разъема (см. рис. 8): для соединения с коммуникационным кабелем (интерфейсный разъем) и PCI-слотом.

Установка системы

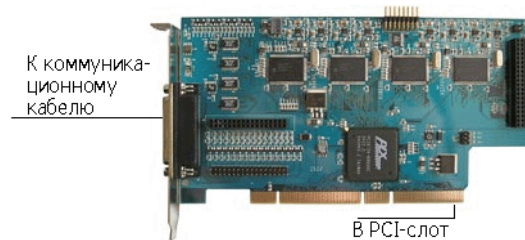


Рис. 8. Расположение разъемов на плате видеозахвата

Возьмите плату так, чтобы PCI-разъем располагался точно над выбранным PCI-слотом материнской платы. Аккуратно надавливая, вставьте PCI-разъем в расположенный под ним слот так, чтобы разъем вошел в слот полностью: до конца и без перекосов. Теперь вход для коммуникационного кабеля будет видим и доступен с обратной стороны корпуса компьютера.

Затем закрепите видеоплату соответствующим винтом. Убедитесь, что она установлена ровно. Повторите вышеописанную последовательность действий установки для каждой дополнительно устанавливаемой платы. Теперь корпус компьютера можно закрыть.

Перед тем как приступить к следующему этапу, подсоедините шнур питания и включите компьютер. Если он не загружается, следуйте приведенному ниже совету. Затем выключите компьютер и отсоедините шнур питания.

2.2.2.2 Подключение видеокамер

Прежде всего подсоедините видеокоммуникационный кабель к видеоплате (с обратной стороны системного блока). Закрепите его, закрутив два винта, расположенные с обоих его концов.

Каждая камера соединяется с BNC-разъемами коммуникационного кабеля своим собственным видеокабелем. Обратите внимание, что на BNC-разъемах коммуникационного кабеля сделаны ярлычки с номерами (см. рис. 9).

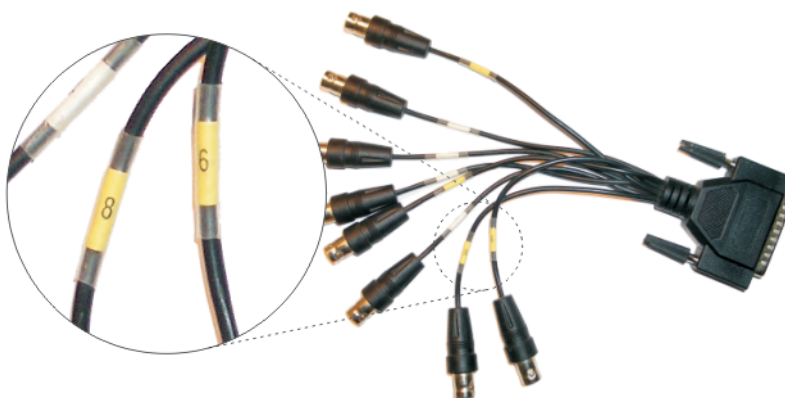


Рис. 9. Коммуникационный кабель и ярлычки BNC-разъемов

Соедините камеры с соответствующими BNC-разъемами. Видеокамеры должны поддерживать тип сигнала PAL или NTSC.

Примечание. Для получения хорошего качества изображения рекомендуется использовать камеры известных фирм, качественные видеокабели и BNC-разъемы.

2.2.2.3 Подключение видео-HUB и IP-камер

SecurOS поддерживает подключение VideoHub™ (сетевые видео-HUB, разработанные компанией ISS), а также других устройств видео-HUB и IP-камер сторонних фирм. Каждое из этих устройств подключается к компьютерам системы SecurOS по протоколу TCP/IP (однако при настройке сети безопасности SecurOS каждое устройство будет виртуально соединено с соответствующим видео-сервером). У каждого из них должен быть свой IP-адрес. Подробную информацию об установке и техническом обслуживании данных устройств видеозахвата можно найти в руководствах к соответствующим моделям.

Примечание. Особенности подключения некоторых IP-камер и видео-HUB сторонних производителей к сети системы SecurOS описаны в разделе [П5.4 Особенности подключения некоторых видеокамер и HUB-устройств](#) на стр. 84

2.2.2.4 Подключение поворотных устройств (купольные камеры)

В систему SecurOS можно интегрировать практически любое поворотное устройство (см. список интегрированных протоколов поворотных устройств в разделе [П6.2 Поворотные устройства](#) на стр. 87). Купольные камеры — это телекамеры, которые подключены к поворотным контроллерам или совмещены с ними.

Процедура подключения состоит из следующих шагов (см. рис. 10):

1. Подключение купольной камеры как обычной телевизионной камеры к видеосерверу (соедините BNC-разъем коммуникационного кабеля с видеокабелем камеры).
2. Подключение поворотного контроллера к последовательному порту видеосервера через интерфейс RS232 и/или RS485 (используйте преобразователь, см. ниже).
3. Определение уникального RS485 ID (адрес, определяемый DIP-переключателями) для каждого поворотного устройства (см. техническую документацию к конкретному поворотному устройству).

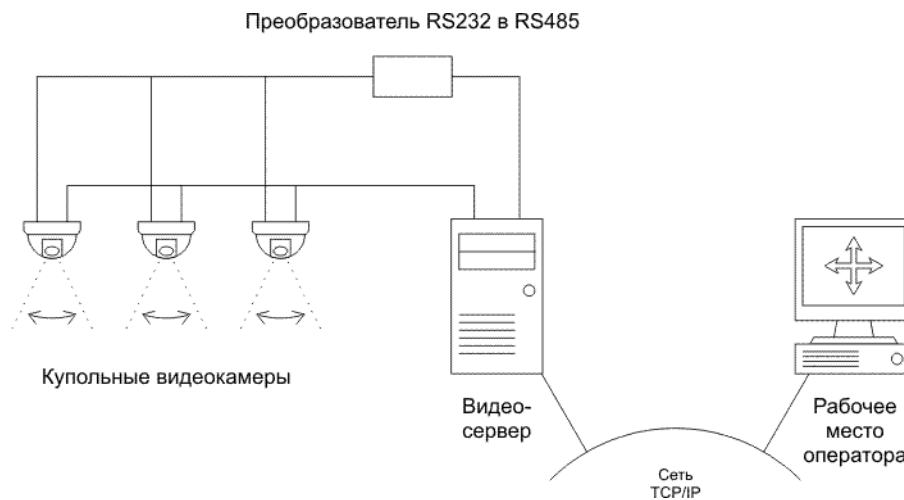


Рис. 10. Схема подключения поворотных устройств

Так как многие поворотные устройства работают по интерфейсу RS232/RS485, то для их подключения к видеосерверу требуется преобразователь RS422/RS485-RS232 (см. рис. 11). Перемычки на преобразователе выставляются в положения: **DCE** и **T-RTS\R-ON**. Преобразователь представляет собой четыре провода (два на прием, два на передачу). В данном случае требуются только два провода, работающие на передачу сигнала. Таким образом, контакты преобразователя **T+** (1) и **T-** (2) соединяются с контактами **R+** и **R-** поворотного устройства соответственно.



Рис. 11. Преобразователь RS422/RS485-RS232

Примечание. Особенности подключения купольных камер к видеосерверам SecurOS и к видео-HUB сторонних производителей в сети системы SecurOS описаны в [Приложение 5. Установка аппаратного обеспечения сторонних производителей](#) на стр. 80

2.2.3 Аудиоподсистема

Аудиоподсистема включает в себя устройства захвата звуковых сигналов — внешние звуковые платы или встроенный аудио интерфейс компьютера. Платы видеозахвата TVISS также могут быть использованы для подключения источников аудиосигнала (см. раздел [Приложение 2. Платы видеозахвата](#) на стр. 52).

Процедура установки звуковой платы аналогична процедуре установки платы видеозахвата, см. раздел [2.2.2.1 Установка видеоплаты](#) на стр. 20. Микрофоны подключаются к выходу **Line In** звуковой платы или компьютера, оборудованного встроенным аудио интерфейсом.

2.2.4 Подсистема оповещения

При необходимости дополнительно установите аудиоплату, подключите активные динамики к выходу **Line Out** аудиоплаты или компьютера, оборудованного встроенным аудио интерфейсом (или используйте выход **Speaker Out** для пассивных динамиков или наушников). Более подробная информация об аудиоплатах содержится в соответствующих руководствах.

Установите модем с поддержкой голосовых сообщений в свободный последовательный порт вашего компьютера и установите драйверы для модема.

2.2.5 Охранно-пожарная подсистема и подсистема контроля доступа

Большинство контроллеров этих подсистем подключаются к серверу приложений через последовательный порт. Некоторые используют протокол RS485 и, соответственно, должны быть подключены через преобразователь RS232–RS485 по аналогии с купольными камерами (см. раздел [2.2.2.4 Подключение поворотных устройств \(купольные камеры\)](#) на стр. 22).

Некоторые контроллеры могут быть напрямую подключены к сети по протоколу TCP/IP. Более подробная информация об определенных видах контроллеров содержится в соответствующих руководствах.

2.2.6 Соединение компьютеров в единую сеть

Все компьютеры системы SecurOS должны быть связаны между собой в единую сеть (либо через LAN — локальную компьютерную сеть, либо через WAN — глобальную сеть Интернет).

В локальной сети используется высокоскоростная технология Ethernet со скоростью передачи данных 10 Мбит/с, 100 Мбит/с (Fast Ethernet) или 1 Гбит/с (Gigabit Ethernet). Производительность системы растет со скоростью передачи данных, что влияет на качество удаленного просмотра видео. Использование такой технологии подходит для сети, приведенной в разделе [2.1.2.2 Централизованное видеонаблюдение](#) на стр. 14.

Глобальная сеть охватывает значительное географическое пространство и включает две или более локальных сетей. Для передачи информации используются коммутируемые и выделенные линии или специальные каналы связи (оптоволоконные или спутниковые). Скорость передачи данных в линиях междоменной связи значительно меньше, чем в локальных сетях. Если требуется про-

смотреть видео из одной локальной сети тогда, как рабочее место оператора находится в другой, то рекомендуется вариант сети, приведенной в разделе [2.1.2.3 Просмотр видео из удаленной сети](#) на стр. 14.

Настроив сетевое подключение, вручную подсоедините к этой сети все компьютеры, на которые будет установлено приложение SecurOS.

Примечание. Перед установкой программного обеспечения SecurOS убедитесь, что каждому компьютеру будущей сети SecurOS (вне зависимости от топологии сети, LAN или WAN) присвоен уникальный IP-адрес.

Чтобы проверить видимость компьютера в сети:

1. Включите компьютер и загрузите операционную систему Windows.
2. Откройте консоль командной строки через меню **Пуск** → **Выполнить**.
3. Введите в поле **Открыть** команду `ipconfig`. Это позволит получить IP-адрес своего компьютера в формате `xxx.xxx.xxx.xxx`.
4. С любого другого компьютера сети откройте консоль командной строки и в поле **Открыть** введите команду `ping xxx.xxx.xxx.xxx` (где `xxx.xxx.xxx.xxx` — полученный на предыдущем шаге IP-адрес). На экране отобразится информация о выполненном запросе (см. строку `time<Nms` для каждого запроса).

2.3 Установка программного обеспечения

В данном разделе описывается процесс установки программного обеспечения на одном сервере (рабочем месте). Для установки (обновления) программного обеспечения SecurOS на многих компьютерах см. [Руководство по автоматизированной установке SecurOS](#).

Внимание! Для установки программы под Windows необходимо обладать правами администратора. Приступайте к установке программного обеспечения только после установки всех необходимых дополнительных устройств на компьютеры и настройки сети.

2.3.1 Содержимое компакт-диска

Установочный компакт-диск SecurOS содержит следующие папки и файлы:

Листинг 1. Содержимое установочного диска SecurOS

```
SecurOS 5.2
  Eula
  Key
    key.iss
  Setup.exe
```

Корневой каталог состоит из одной или нескольких папок (например, SecurOS 5.2, где 5.2 — версия программного продукта, которая может отличаться от указанной на компакт-диске).

Примечание. Лицензионный ключ можно получить по электронной почте (см. раздел [Обращение за технической поддержкой](#) на стр. 6).

2.3.2 Процедура установки

1. Вставьте компакт-диск с программным обеспечением SecurOS в дисковод компьютера и запустите файл `Setup.exe`. В появившемся диалоговом окне выберите язык программы установки и нажмите кнопку **ОК**. Появится окно Мастера установки (см. рис. 12).

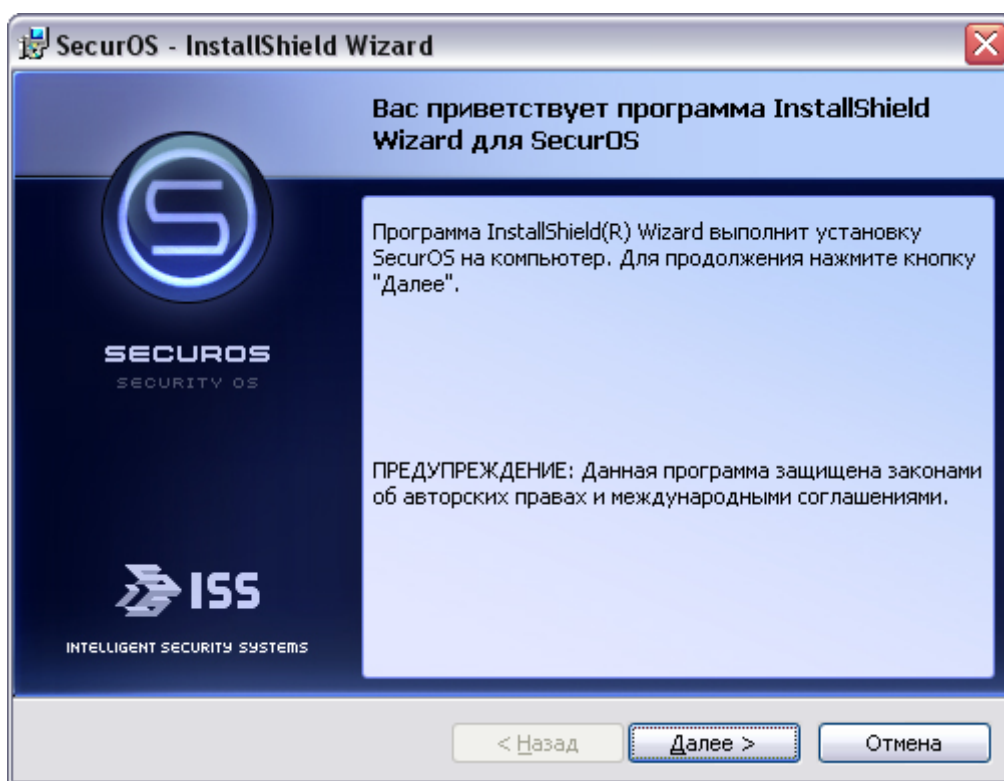


Рис. 12. Приветствие программы Мастера установки

С помощью программы Мастера установки можно указать требования к системе безопасности перед копированием файлов. Можно выйти из программы и отменить установку на любом шаге без каких-либо последствий. При нажатии кнопки **Назад** произойдет возврат к предыдущему шагу установки. Нажмите кнопку **Далее** для продолжения.

*При запуске Мастера установки появляется диалоговое окно **Обслуживание программ** с возможностью выбора следующих опций: Изменить, Исправить и Удалить. Что это означает?*

Это означает, что программное обеспечение SecurOS уже установлено на этом компьютере или предыдущая версия была удалена некорректно (см. раздел [2.4 Обновление программного обеспечения](#) на стр. 35). Нажмите кнопку **Далее** для продолжения установки программы SecurOS или кнопку **Отмена** для выхода из программы Мастера установки.

Примечание. Для работы SecurOS может потребоваться дополнительное программное обеспечение, установка которого будет предложена (см. рис. 13). Нажмите кнопку **Установить** для начала установки.

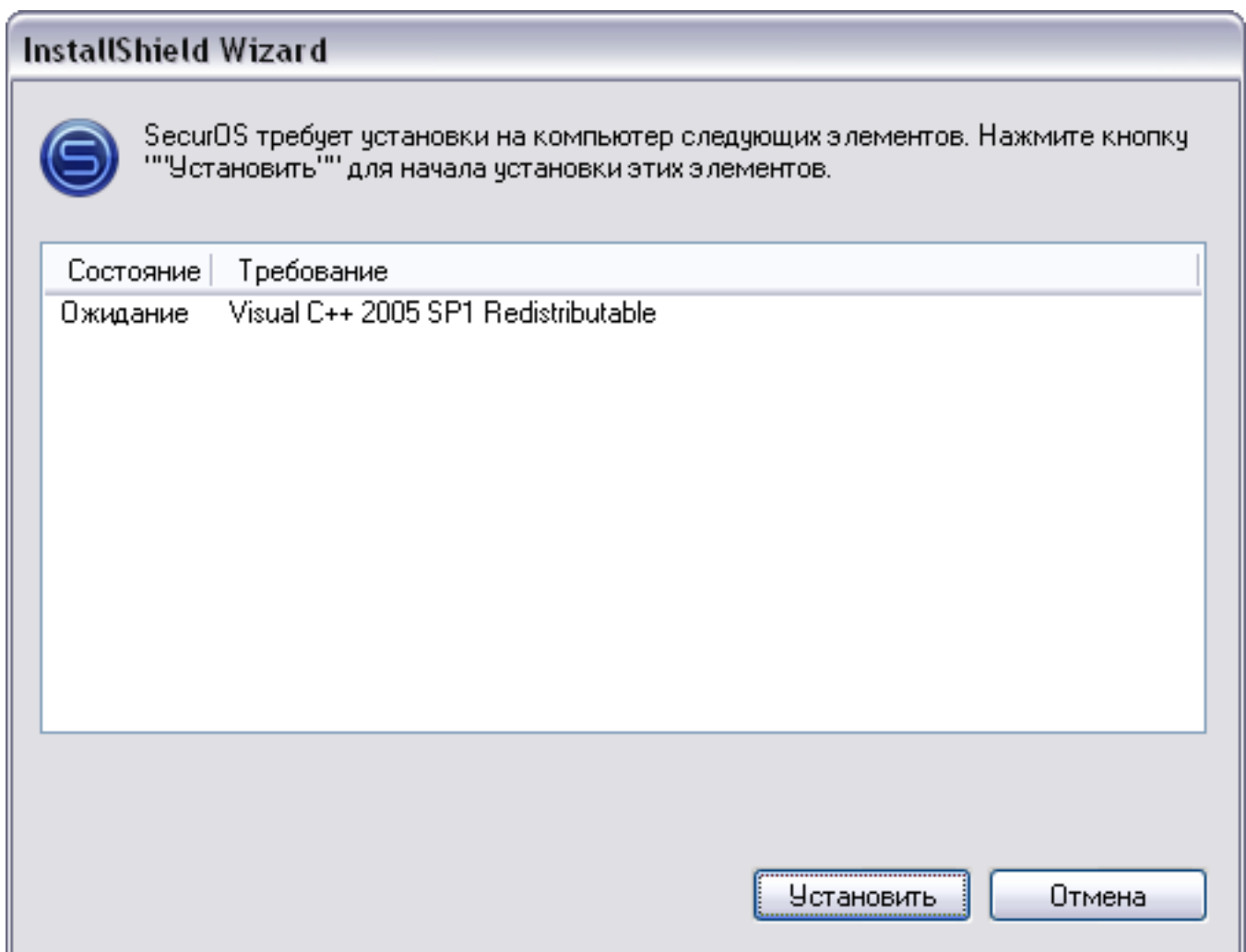


Рис. 13. Установка дополнительного программного обеспечения

2. Внимательно прочтите лицензионное соглашение. В случае принятия условий соглашения выберите **Я принимаю условия соглашения** и нажмите кнопку **Далее** для продолжения. В случае непринятия условий соглашения нажмите кнопку **Отмена** для выхода из программы Мастера установки.
3. Введите свое имя и название организации и нажмите кнопку **Далее** для продолжения.

4. В новом окне (см. рис. 14) выберите из списка необходимый вид установки для данного компьютера (см. раздел 1.3 [Виды серверов и рабочих мест](#) на стр. 9). Помните, что видеосервер должен быть оборудован видеоплатой, а на другие компьютеры (кроме рабочего места оператора) должны быть установлены ключи Guardant. Нажмите кнопку **Далее** для продолжения. Если выбран вид установки **Рабочее место оператора**, то см. п. 6.

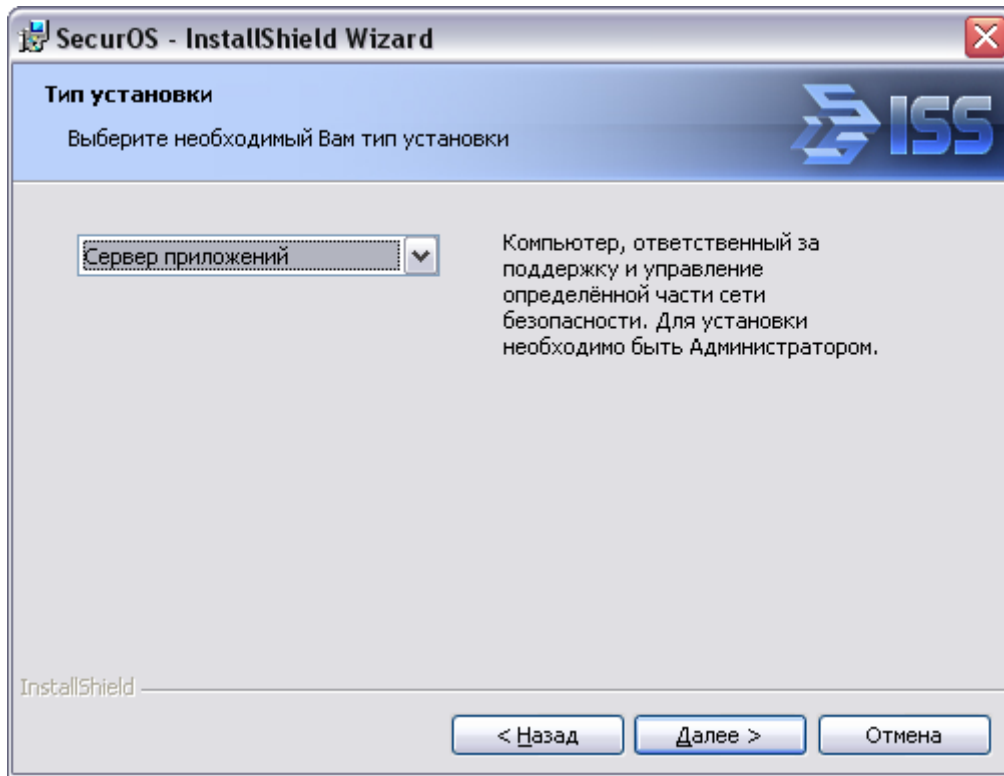


Рис. 14. Выбор типа установки

5. Нажмите кнопку **Поиск** и укажите папку, содержащую файл лицензионного ключа SecurOS (key.iss). Обычно он находится в подкаталоге \SecurOS установочного диска. Можно оставить поле пустым, но тогда после установки нужно будет вручную скопировать файл лицензионного ключа key.iss в корневой каталог SecurOS.

*Не удастся найти файл key.iss на установочном диске / установочный диск потерян.
Как получить этот файл?*

Обратитесь к системному интегратору или в Службу технической поддержки компании ISS (см. раздел [Обращение за технической поддержкой](#) на стр. 6).

6. Укажите папку, в которую следует установить SecurOS. По умолчанию система предложит папку C:\Program Files\ISS\SecurOS. Чтобы выбрать другую папку, нажмите кнопку **Изменить** или укажите путь вручную. Нажмите кнопку **Далее** для продолжения.

7. Если новая версия SecurOS устанавливается на сервере приложений поверх старой, выберите из списка действие, которое следует выполнить с текущими базами данных SecurOS (см. рис. 15):

- **Пересоздать базы данных** — база данных будет переписана, существующая информация будет удалена. Выберите это значение только при полной уверенности, что старые настройки не понадобятся;
- **Использовать существующие базы данных** — будет использоваться уже существующая база данных PostgreSQL и текущие настройки сервера приложений, которые остались от предыдущей установки SecurOS на этом компьютере. Это значение рекомендуется и выбрано по умолчанию.

Примечание. Для корректной работы базы данных предыдущая и текущая версии SecurOS должны быть согласованы.

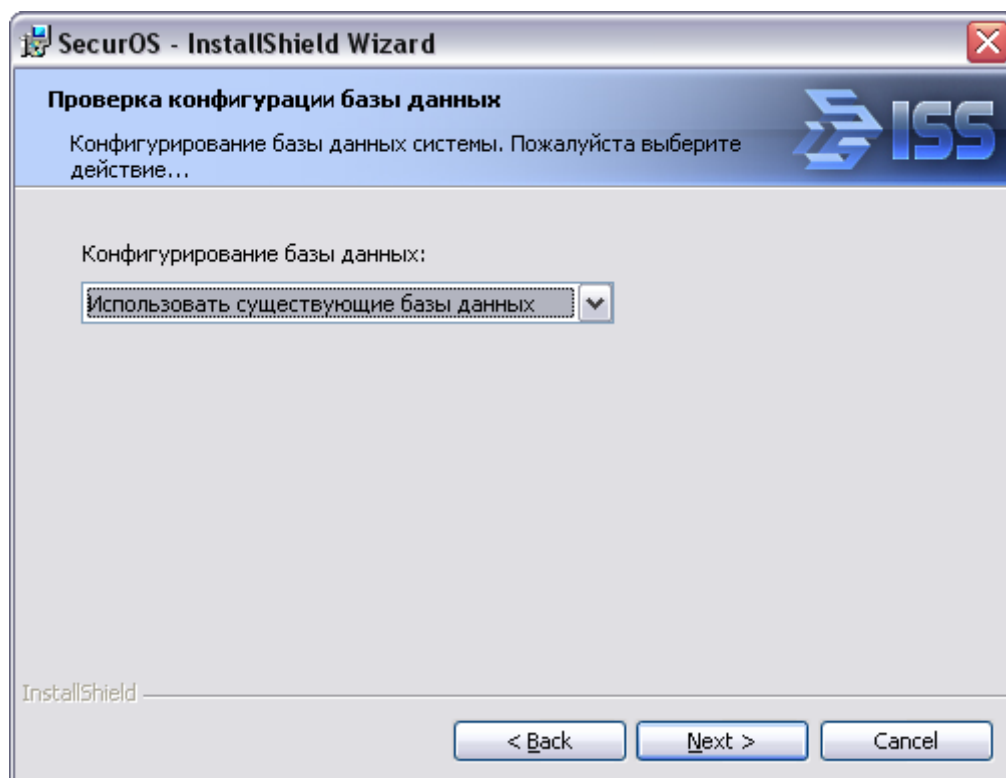


Рис. 15. Определение конфигурации базы данных системы

Внимание! В целях предосторожности при обновлении программного обеспечения SecurOS рекомендуется делать резервную копию всей папки SecurOS.

Нажмите кнопку **Далее** для продолжения.

8. Если SecurOS устанавливается впервые или в п. 7 было выбрано значение Пересоздать базы данных, выберите режим установки базы данных (см. рис. 16):

- Сервер — будет использоваться локальная база данных;
- Клиент — база данных будет подключаться с удаленного сервера.

Нажмите кнопку **Далее** для продолжения. Если выбран режим Клиент, см. п. 11.

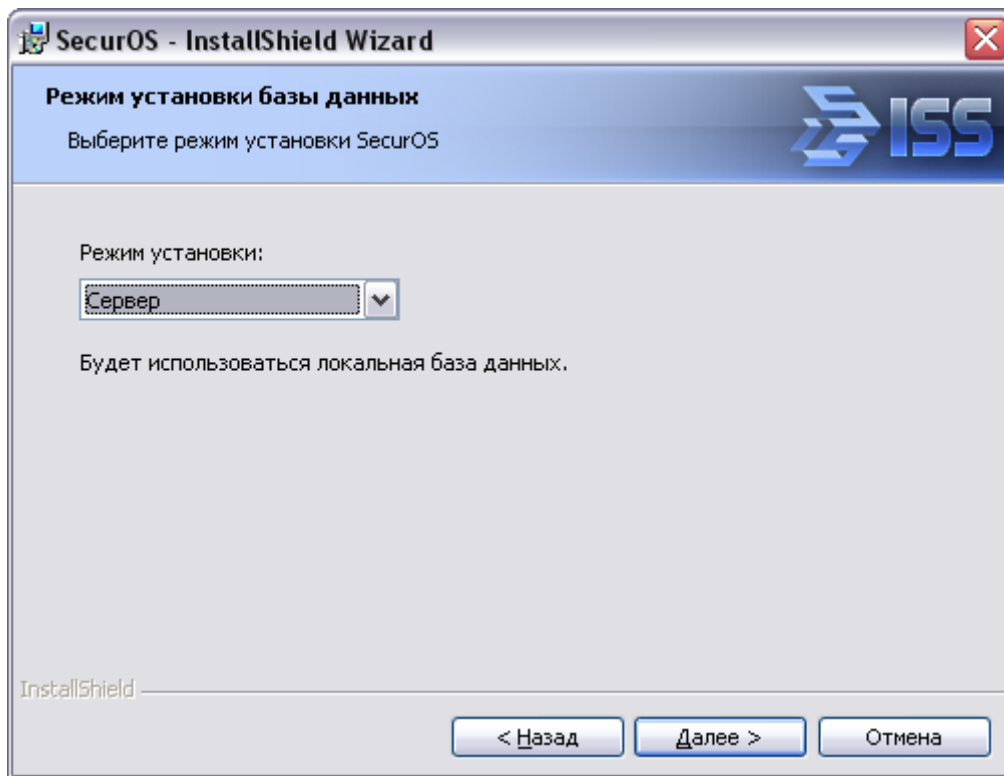


Рис. 16. Выбор режима установки

9. Если SecurOS не был ранее установлен на этом компьютере, или была установлена версия под управлением СУБД PostgreSQL 8.3, то появится окно определения параметров установки СУБД (рис. 17), в противном случае см. п. 10.

Внимание! Данная версия SecurOS работает только с СУБД PostgreSQL 8.3.

Укажите следующие параметры установки СУБД PostgreSQL:

- учетную запись и пароль администратора СУБД PostgreSQL (с подтверждением пароля);

- папку, в которую будет установлена СУБД PostgreSQL. По умолчанию предлагается установить в C:\Program Files\PostgreSQL\8.3. Для выбора другой папки нажмите кнопку **Обзор** или введите вручную;

Внимание! Если на компьютере была установлена СУБД PostgreSQL 8.3, укажите папку, отличную от корневой папки PostgreSQL 8.3.

- папку, в которой будут храниться файлы баз данных СУБД PostgreSQL. По умолчанию предлагается установить в C:\Program Files\PostgreSQL\8.3\Data. Для выбора другой папки нажмите кнопку **Обзор** или введите вручную.

Внимание! Если на компьютере была установлена СУБД PostgreSQL 8.3, укажите папку, отличную от папки с файлами баз данных PostgreSQL 8.3.

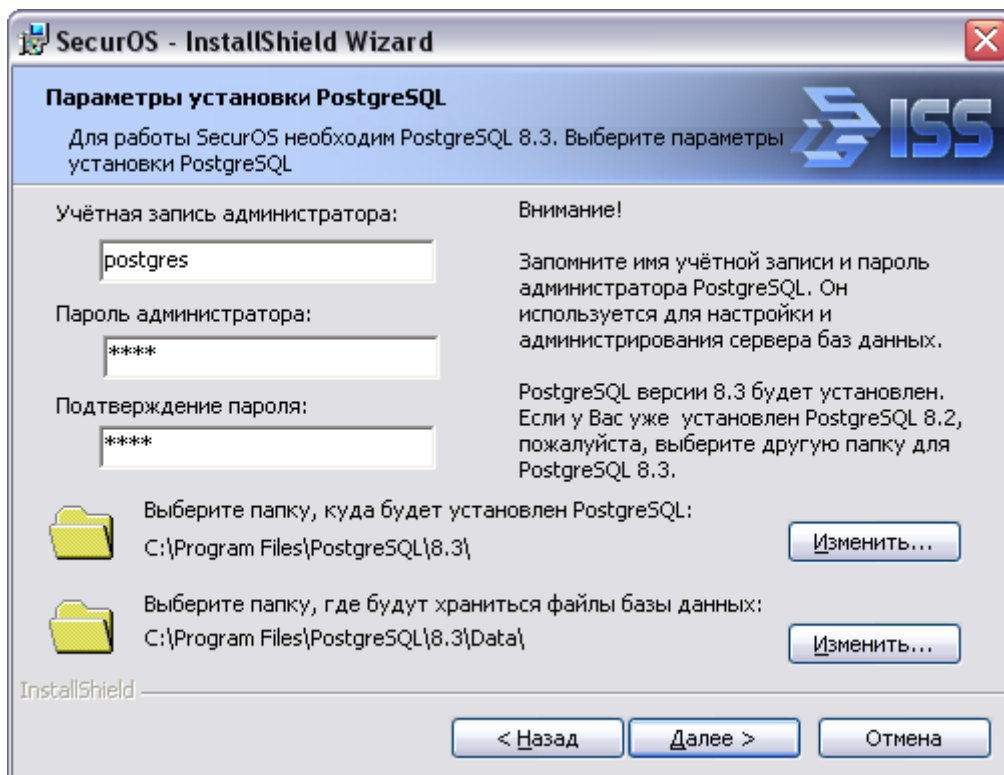


Рис. 17. Определение параметров установки СУБД PostgreSQL

Внимание! Запомните учетную запись и пароль администратора СУБД PostgreSQL. Эти параметры используются для настройки и администрирования сервера баз данных.

Нажмите кнопку **Далее** для продолжения.

10. Определите параметры базы данных (см. рис. 18). Укажите имя новой базы данных, а также учетную запись и пароль (с подтверждением) для соединения с базой данных. Если SecurOS был ранее установлен в режиме Сервер на этом компьютере и планируется использование существующей базы данных, то введите имя и учетную запись существующей базы. Нажмите кнопку **Далее** для продолжения.

SecurOS - InstallShield Wizard

База данных

Задайте параметры для базы данных

Имя базы данных:

securos

Учётная запись пользователя:

postgres

Пароль пользователя:

Подтверждение пароля:

Вы можете указать:

- имя и учётную запись существующей базы данных (если SecurOS был ранее установлен на этом компьютере в серверном варианте)
- либо
- имя и учётную запись новой базы данных.

☐ Данный компьютер является контроллером домена или Active Directory

InstallShield

< Назад Далее > Отмена

Рис. 18. Определение параметров новой базы данных

11. Выберите язык интерфейса SecurOS. Выбранный язык должен быть прописан в лицензионном ключе (key.iss), иначе программа не будет запускаться. Нажмите кнопку **Далее** для продолжения.
12. Выберите установку дополнительных драйверов для видеоплат и драйверов электронных ключей Guardant. Если в п. 4 было выбрано значение **Видео-сервер**, выберите установку драйверов видеоплат, установленных на компьютере (см. рис. 19), и нажмите кнопку **Далее** для продолжения. Если в компьютере используется электронный ключ Guardant, выберите установку драйверов Guardant.

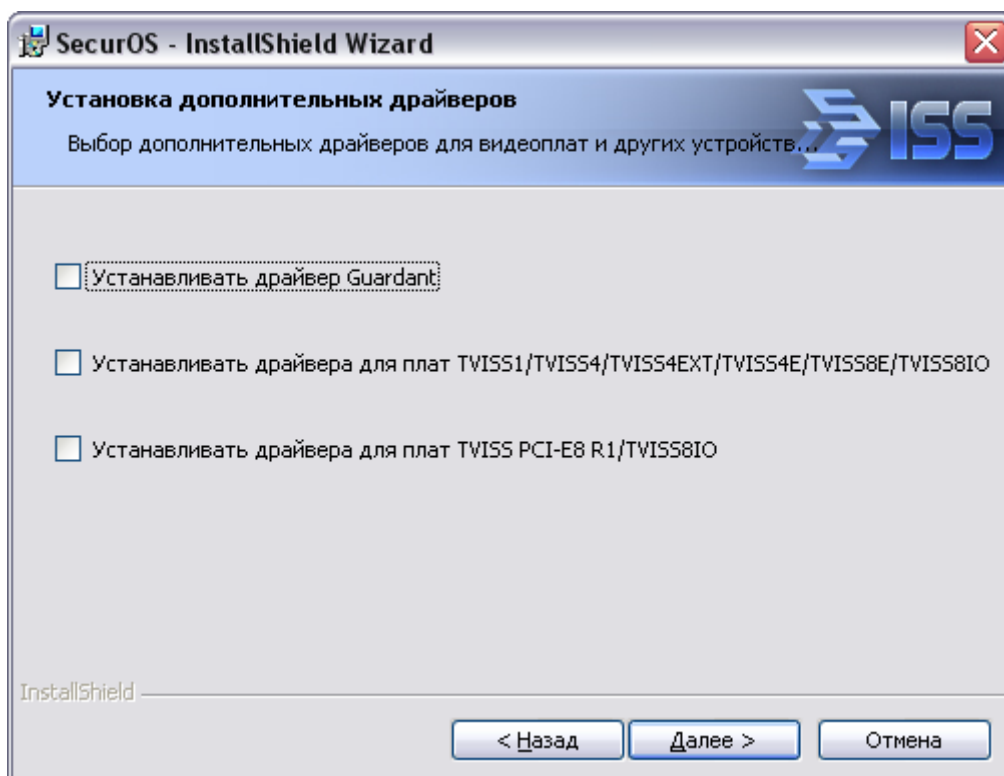


Рис. 19. Выбор дополнительных драйверов

13. Активируйте поле **Создать ярлык на Рабочем столе**, чтобы создать на рабочем столе иконку для запуска SecurOS, и/или поле **Создать ярлык в Панели быстрого запуска**, чтобы создать на панели задач дополнительную иконку для запуска SecurOS. Нажмите кнопку **Далее** для продолжения.
14. Просмотрите список выбранных установок: для внесения изменений используйте кнопку **Назад**; если все верно, нажмите кнопку **Установить** для запуска процесса установки.
15. По окончании процесса установки появится окно завершения. Нажмите кнопку **Завершить** для выхода из программы Мастера установки.

Примечание. Программа установки может предложить перезагрузить компьютер (если были установлены драйверы для плат видеозахвата). Если перезагрузка не будет выполнена сразу, необходимо перезагрузить компьютер перед первым запуском SecurOS.

2.4 Обновление программного обеспечения

Компания ISS постоянно выпускает новые версии программного обеспечения SecurOS. Для обновления необходимо установить новую версию поверх устаревшей (в тот же каталог), см. раздел [2.3 Установка программного обеспечения](#) на стр. 25. При обновлении сохраняются текущие настройки программного обеспечения SecurOS, если при настройке базы данных конфигурации не было выбрано значение **Переписать** (см. п. 7 раздела [2.3.2 Процедура установки](#) на стр. 26).

Примечание. При обновлении программного обеспечения SecurOS рекомендуется делать резервную копию всей папки \SecurOS.

2.5 Удаление программного обеспечения

Удаление программы SecurOS происходит в два этапа:

- удаление программного обеспечения через InstallShield Wizard;
- удаление видео-, аудиоархивов и базы данных конфигурации (по желанию).

Для удаления программного обеспечения откройте окно InstallShield Wizard (**Пуск** → **Настройки** → **Панель управления** → **Установка и удаление программ**). Выберите приложение SecurOS и нажмите кнопку **Удалить**. InstallShield Wizard запустит процедуру удаления.

Примечание. Не рекомендуется самостоятельно удалять файлы программы SecurOS, так как это может дестабилизировать систему.

После удаления программного обеспечения, возможно, понадобится удалить все видео- и аудио-архивы, а также базу данных конфигурации (InstallShield Wizard эти файлы не удаляет). Таким образом, необходимо это сделать вручную: удалите каталог SecurOS (обычно, C:\SecurOS) для удаления базы данных и каталоги \Video и \Audio (обычно находятся на одном или нескольких жестких дисках в корневом каталоге, например C:\Video, C:\Audio, D:\Video, D:\Audio) — для архивов.

3. Запуск системы

В этом разделе описывается процесс запуска программного обеспечения сервера приложений. Запуск рабочего места администратора полностью аналогичен. Запуск и настройка программного обеспечения рабочего места оператора см. [Руководство пользователя SecurOS](#).

Внимание! После установки ПО SecurOS и СУБД PostgreSQL в ОС Windows создается учетная запись `postgres`. Для настройки системы SecurOS используйте учетную запись Windows администратора, но не `postgres`.

Внимание! Срок действия пароля учетной записи Windows `postgres` не должен быть ограничен, в противном случае через некоторое время работа SecurOS будет блокирована. Откройте **Панель управления**, нажмите на элемент **Учетные записи пользователей**, выберите вкладку **Дополнительно** и нажмите кнопку **Дополнительно**. В окне **Локальные пользователи и группы** откройте слева папку **Пользователи**, нажмите на имя пользователя **Postgres** правой кнопкой мыши и выберите **Свойства**. Активируйте опцию **Срок действия пароля не ограничен**.

Внимание! Во избежание блокирования работы системы SecurOS необходимо, чтобы отсутствовал срок действия пароля администратора PostgreSQL `postgres`. Запустите утилиту PostgreSQL **PgAdmin III** и проверьте поле **Account expires** для учетной записи `postgres` администратора базы данных SecurOS. Поле должно быть пустым, в ином случае нажмите правой кнопкой мыши на имя учетной записи и выберите **Properties**, затем укажите значение 0 в поле **Account expires**.

3.1 Запуск на сервере / рабочем месте администратора

Для запуска SecurOS на сервере приложений (рабочем месте администратора) дважды нажмите значок программы SecurOS на рабочем столе или выберите из меню **Пуск** → **Программы** → **SecurOS**. Появится окно процесса инициализации.

Примечание. Для автоматического запуска SecurOS при загрузке системы необходимо выполнить дополнительные настройки Windows (см. раздел [П7.3 Утилита ISS Startup Configuration](#) на стр. 93).

При запуске SecurOS появляется сообщение об ошибке. Что делать?

Список возможных ошибок и советы по их устранению см. в разделе [Приложение 1. Часто задаваемые вопросы](#) на стр. 49.

3.1.1 Первый запуск

При первом запуске программы SecurOS запустится Мастер первоначальной настройки, который поможет создать начальную системную конфигурацию сети SecurOS.

1. Активируйте в списке на начальном экране (см. рис. 20) поле, соответствующее одному из возможных сценариев работы Мастера первоначальной настройки:

- **Настроить SecurOS с помощью Мастера первого запуска** — настройка параметров системы SecurOS на данном компьютере (диски для хранения архива, параметры IP-камер и сетевых видео-HUB, имена компьютеров рабочих мест оператора), см. пп. 2–7;
- **Присоединиться к существующей сети безопасности** — подключение к уже существующей сети безопасности SecurOS, см. п. 8;
- **Импортировать конфигурационный файл** — импорт файла с ранее сохраненной конфигурацией SecurOS, см. п. 9;
- **Запуск с пустой базой данных** — запуск SecurOS с настройками по умолчанию и минимальной конфигурацией, см. п. 10.

Нажмите кнопку **Далее** для продолжения (рис. 20). Также можно вернуться на любой предыдущий шаг настройки для изменения настроек, нажав кнопку **Назад**, или отменить работу Мастера, нажав кнопку **Отмена**.

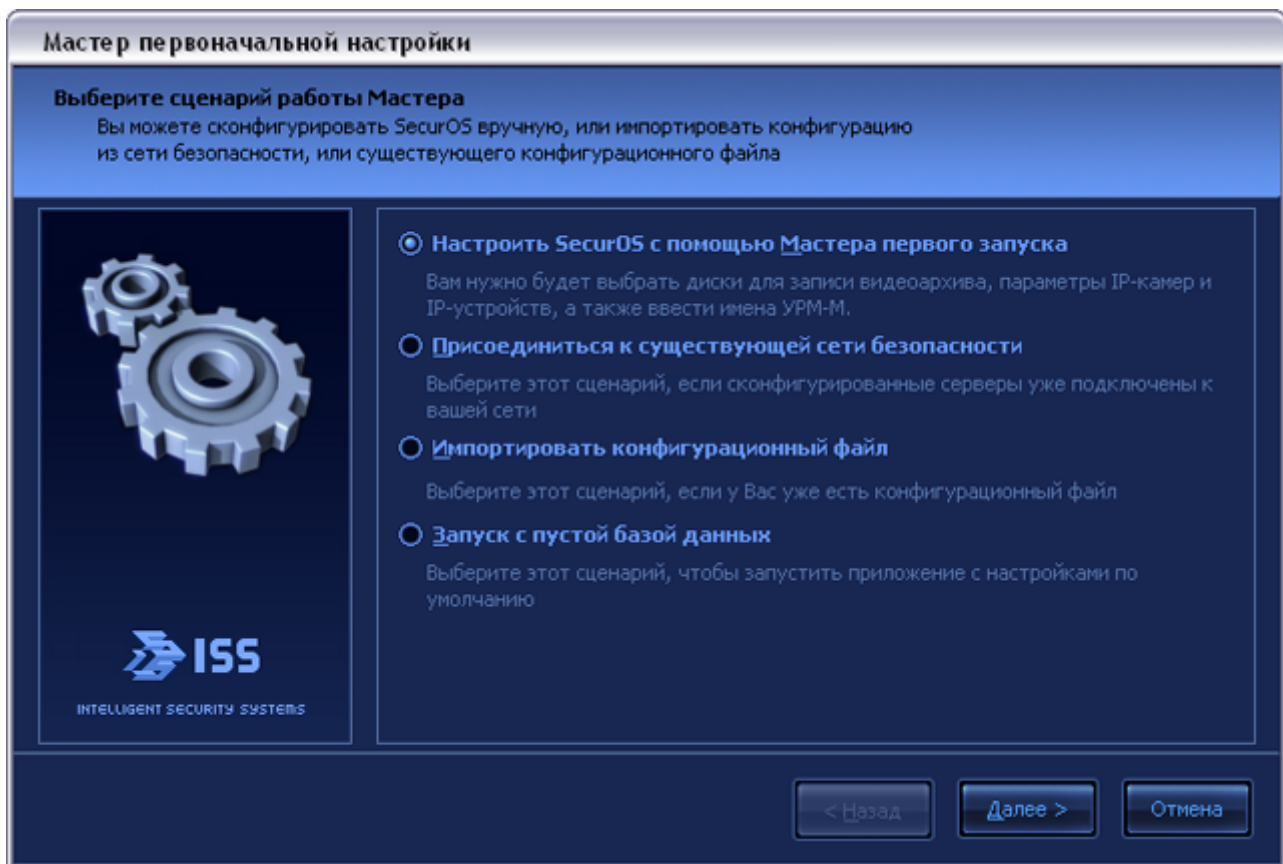


Рис. 20. Мастер первоначальной настройки: выбор сценария работы

2. Если выбран тип сценария **Настроить SecurOS с помощью Мастера первого запуска**, в окне Мастера первоначальной настройки появится краткая информация о возможностях Мастера. Нажмите кнопку **Далее** для продолжения (рис. 21).

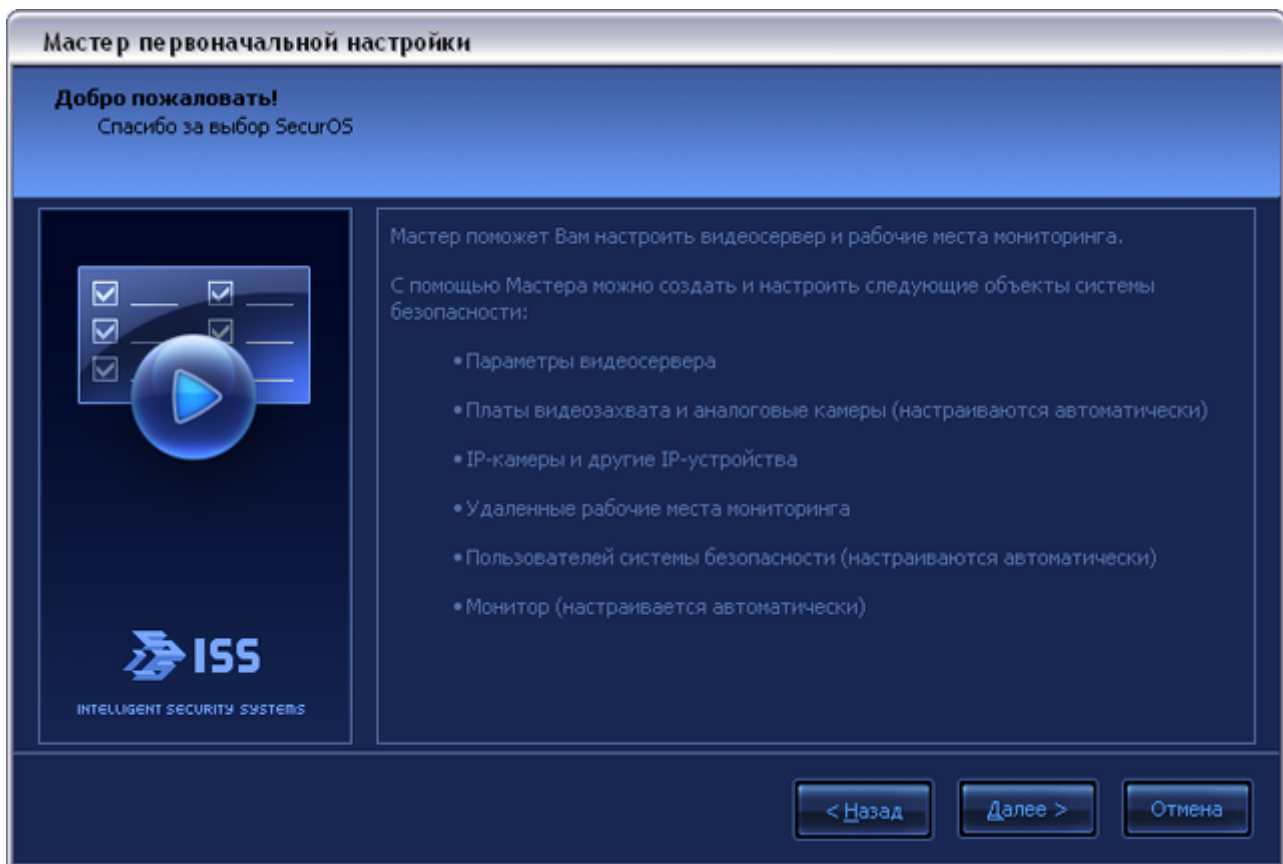


Рис. 21. Мастер первоначальной настройки: начало

3. В окне Мастера первоначальной настройки появится информация о текущих параметрах конфигурации, которые установлены в файле ключа (рис. 22).

Отображаются следующие данные:

- число доступных видео-серверов;
- число удаленных рабочих станций оператора;
- число и тип поддерживаемых карт видеозахвата;
- число доступных аналоговых камер в конфигурации;
- число и тип доступных IP-камер;
- число доступных пользователей.

Нажмите кнопку **Далее** для продолжения.

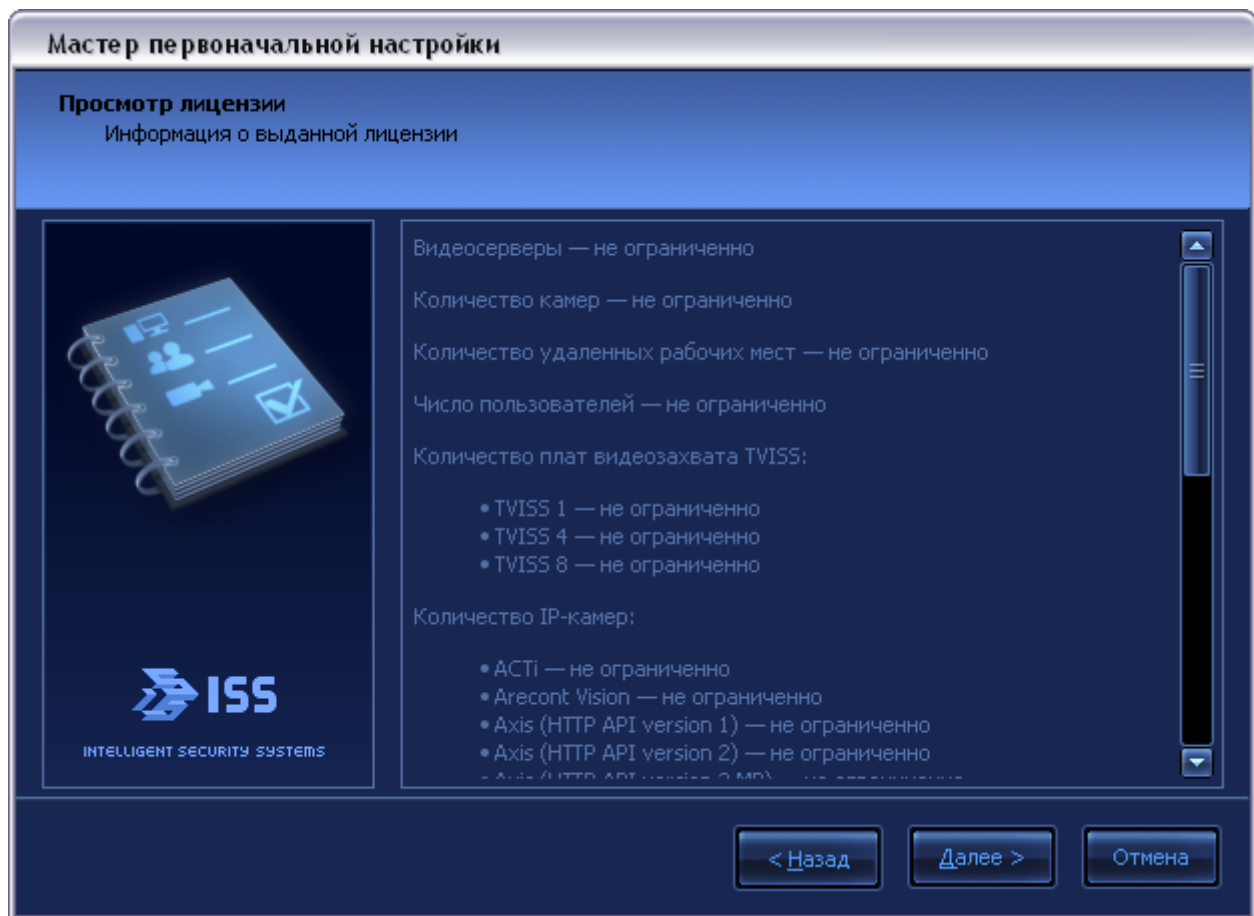


Рис. 22. Мастер первоначальной настройки: информация о текущей конфигурации

4. В новом окне (см. рис. 24) укажите имя компьютера в поле **Введите имя компьютера**.

Внимание! Если указать в имени компьютера недопустимый символ, появится окно предупреждения со списком недопустимых символов (см. рис. 23).

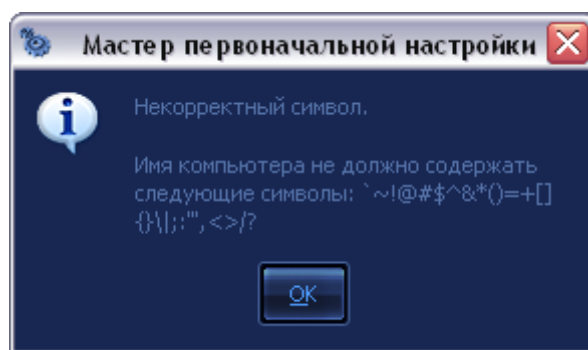


Рис. 23. Мастер первоначальной настройки: предупреждение о некорректном символе в имени компьютера

Активируйте поля, соответствующие дискам, которые будут использоваться для видеоархива, в списке ниже. Нажмите кнопку **Далее** для продолжения.

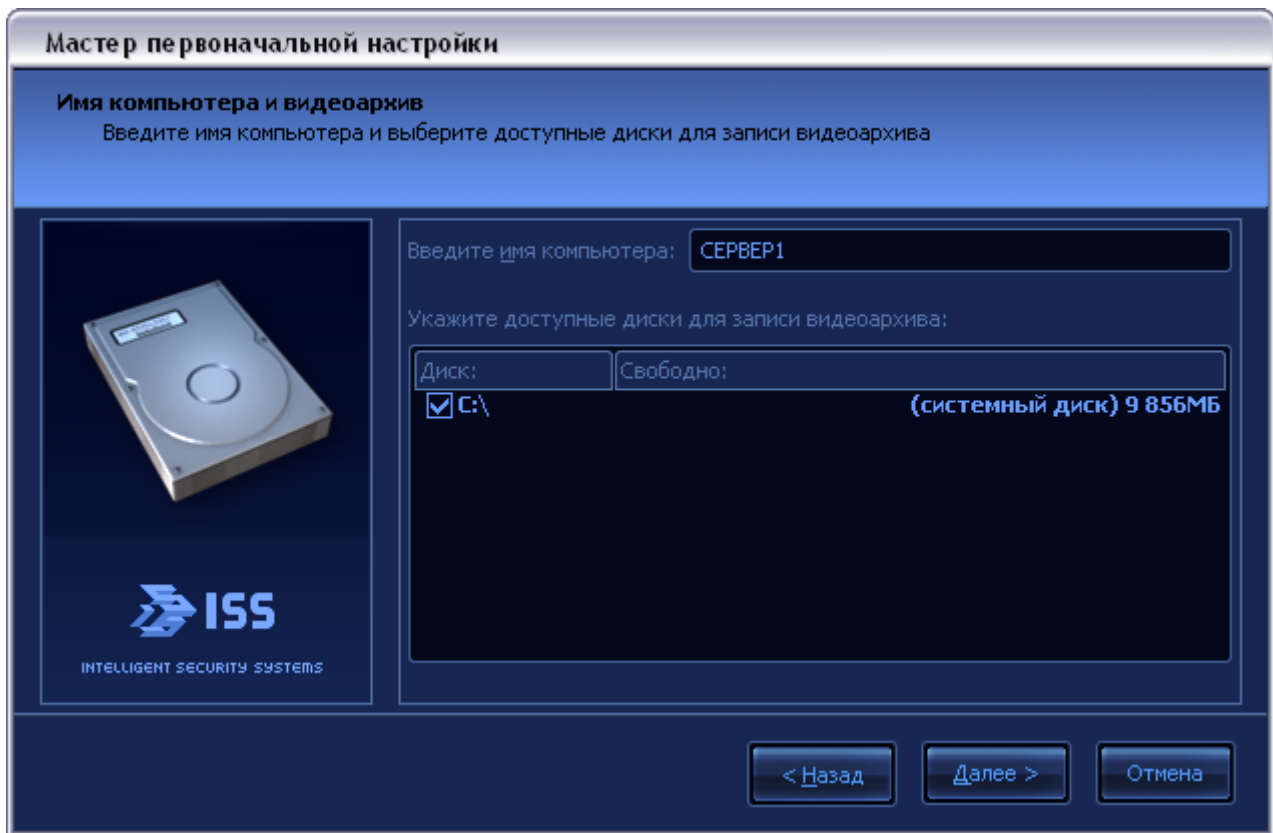


Рис. 24. Мастер первоначальной настройки: информация об имени компьютера и дисках видеоархива

5. На панели Мастера появится таблица для добавления списка всех доступных IP-камер и видео-хабов в системной сети (рис. 25).

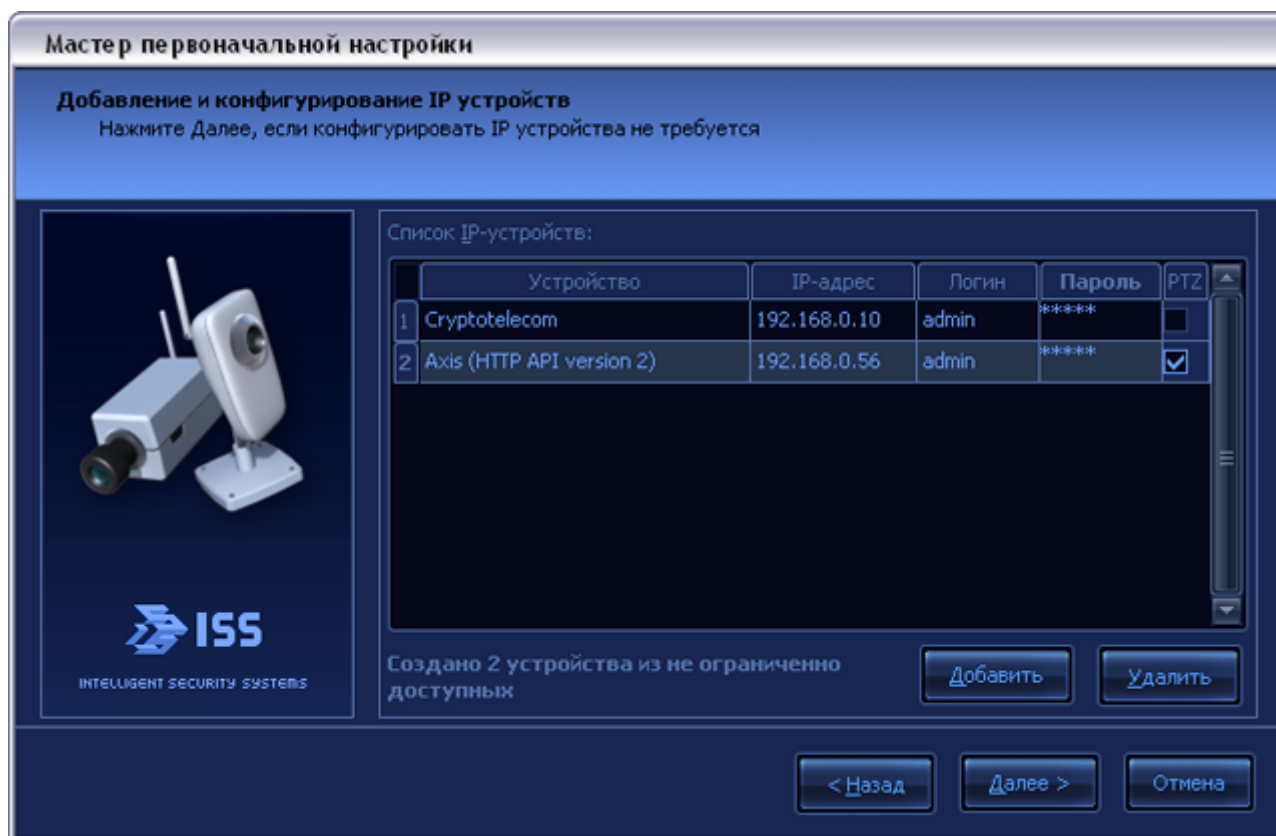


Рис. 25. Мастер первоначальной настройки: информация о IP-камерах

Чтобы добавить устройство в таблицу:

- Нажмите кнопку **Добавить**. Пустая строка будет добавлена в таблицу.
- Дважды нажмите на столбец **Устройство** текущей строки и выберите название устройства из выпадающего списка.
- Укажите IP-адрес выбранного устройства в системной сети в столбце **IP-адрес** текущей строки.
- Укажите логин и пароль доступа к устройству в полях **Логин** и **Пароль**.

Примечание. Пароль будет замаскирован звездочками.

- Активируйте поле в столбце **PTZ**, если устройство оборудовано контроллером телеметрии (поворотным устройством).

Примечание. Для объектов *Камера*, созданных Мастером первоначальной настройки для устройств видеозахвата, параметры «горячей» записи устанавливаются по умолчанию как 5 секунд для пред-записи и 5 секунд для пост-записи.

Чтобы удалить устройство из таблицы, выделите строку, соответствующую устройству, и нажмите кнопку **Удалить**.

После заполнения таблицы нажмите кнопку **Далее** для продолжения.

6. Добавьте имена удаленных рабочих мест оператора в список рабочих мест оператора (рис. 26).

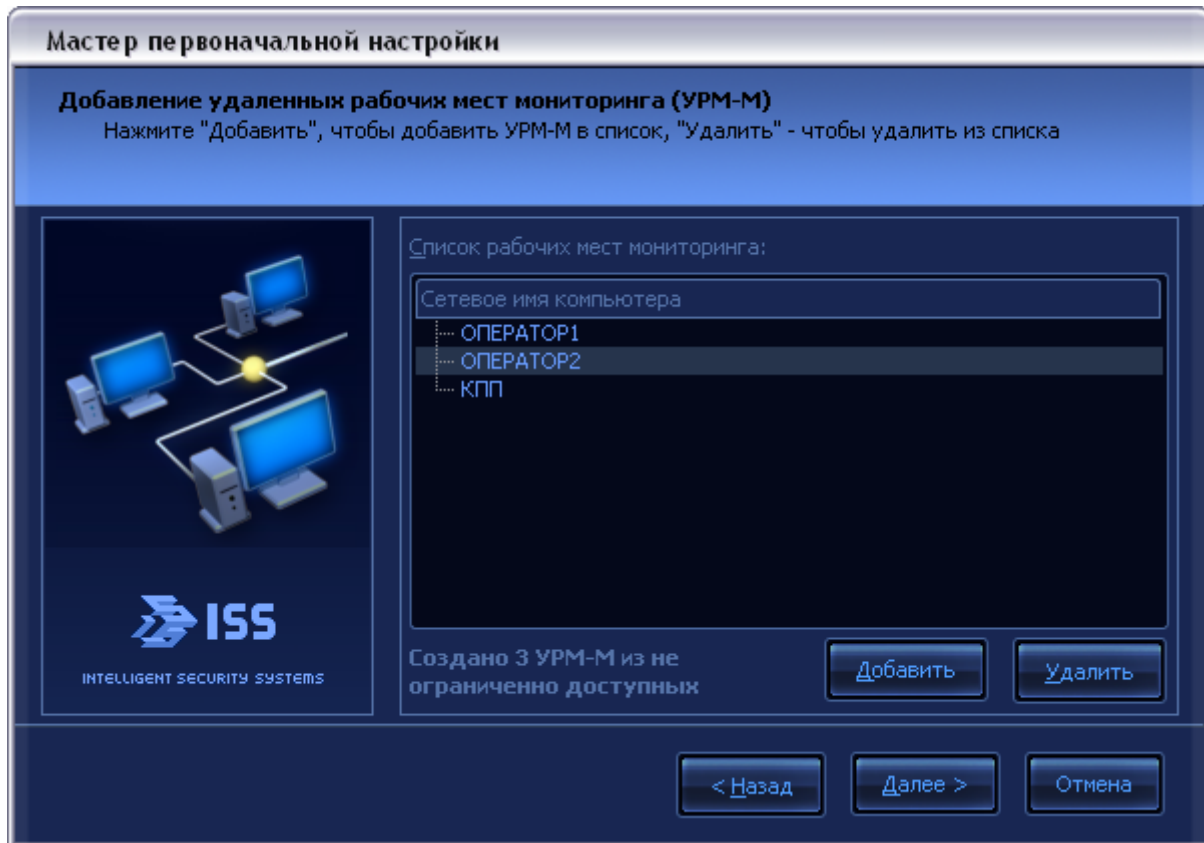


Рис. 26. Мастер первоначальной настройки: список рабочих мест оператора

Чтобы добавить рабочее место:

- а) Нажмите кнопку **Добавить**. Пустая строка будет добавлена в список.
- б) Укажите имя рабочего места в строке и нажмите клавишу **Enter**, или нажмите кнопку [...] для добавления существующего компьютера. Появится окно выбора компьютера со списком доступных компьютеров в сети (см. рис. 27). Выберите компьютер из списка и нажмите кнопку **ОК**.

Чтобы удалить компьютер из списка, выделите строку, соответствующую компьютеру, и нажмите кнопку **Удалить**.

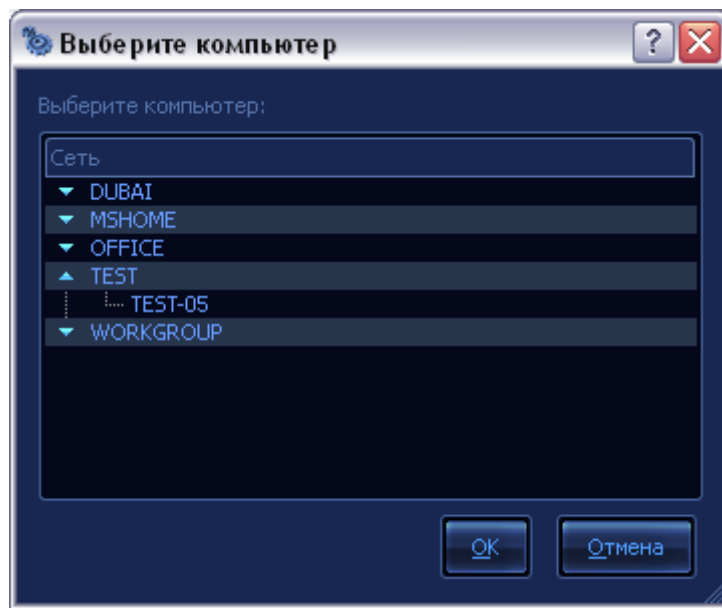


Рис. 27. Мастер первоначальной настройки: окно выбора компьютера

Внимание! Если указать в имени компьютера недопустимый символ, появится окно предупреждения со списком недопустимых символов (см. рис. 23).

После заполнения таблицы нажмите кнопку **Далее** для продолжения.

- Внимательно просмотрите суммарную информацию о конфигурации системы. Если вся информация корректна, нажмите кнопку **Готово** для завершения мастера настройки, создания и сохранения новой конфигурации, и автоматического запуска системы SecurOS с созданной конфигурацией.

Примечание. По умолчанию, в системной конфигурации создаются две учетных записи пользователя и одна учетная запись администратора: `operator1` (пароль `operator1`), `operator2` (пароль `operator2`), и `root` (пароль `securos5`), соответственно.

8. Если выбран тип сценария **Присоединиться к существующей сети безопасности**, появится окно выбора конфигурационного (ведущего) сервера для подключения к уже существующей сети безопасности SecurOS (см. рис. 28).

Чтобы запустить поиск серверов в сети, нажмите кнопку **Начать поиск** (или **Обновить список**). В списке ниже появятся доступные серверы сети SecurOS.

Выделите в списке сервер для подключения. Выбранный сервер появится в поле **Имя или IP-адрес конфигурационного сервера**.

Внимание! В целях безопасности необходимо зарегистрировать свой компьютер в конфигурации сети SecurOS, к которой производится подключение (процедура регистрации компьютера в сети безопасности SecurOS описана в [Руководстве администратора SecurOS](#)). Укажите данный компьютер в списке **Сервера для подключения** в настройках сервера сети безопасности, который будет ведущим (см. [Руководство администратора SecurOS](#)). Затем можно подключить ведущий сервер приложений. Он производит авторизацию подключаемого компьютера и передает ему информацию, необходимую для начала работы.

Далее нажмите кнопку **Зафиксировать**. При успешном соединении и авторизации база данных будет скопирована с сервера на компьютер.

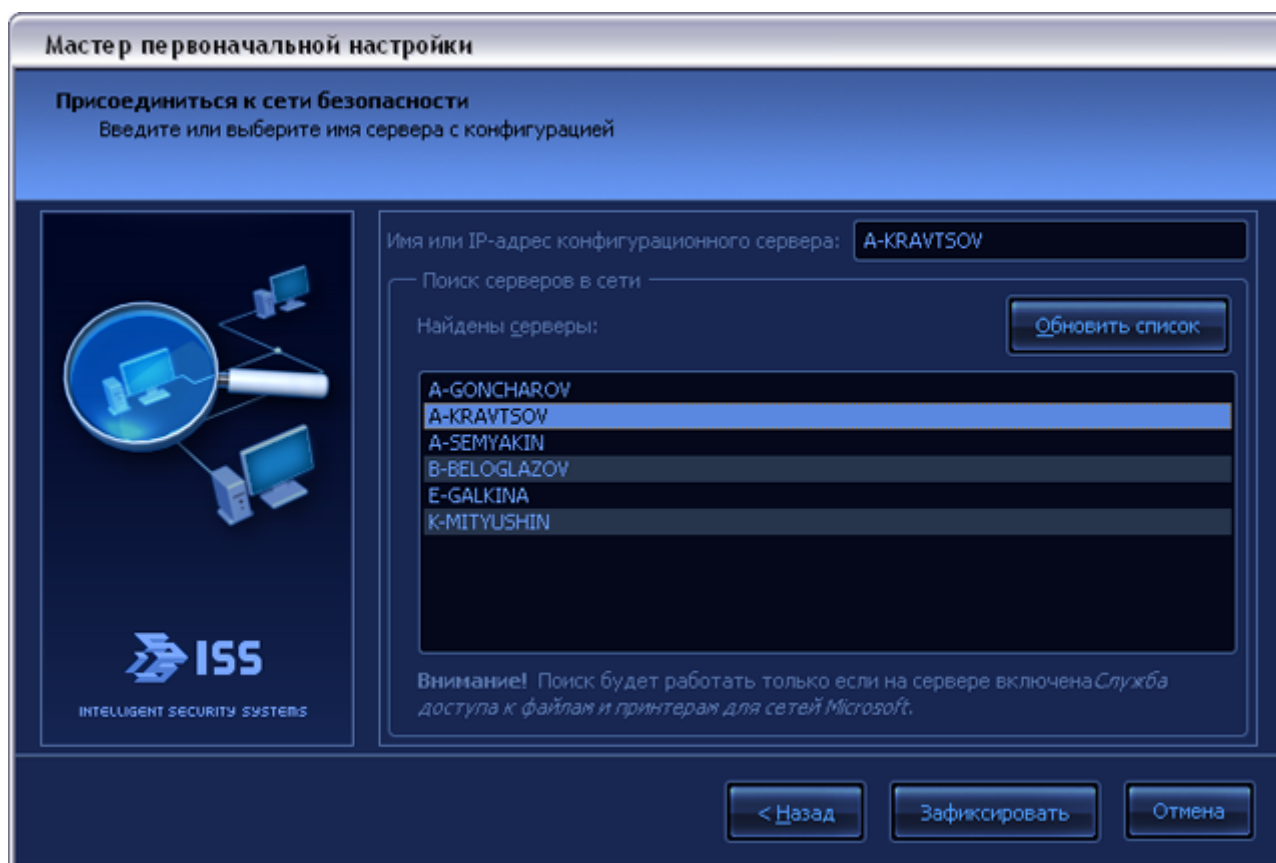


Рис. 28. Мастер первоначальной настройки: подключение к существующей сети безопасности

9. Если выбран тип сценария **Импортировать конфигурационный файл**, появится окно выбора предварительно сохраненного файла конфигурации (см. рис. 29). Нажмите кнопку [...] и выберите файл конфигурации в стандартном диалоговом окне. Нажмите кнопку **Готово** для завершения мастера настройки, импорта файла конфигурации, и автоматического запуска системы SecurOS с импортированной конфигурацией.

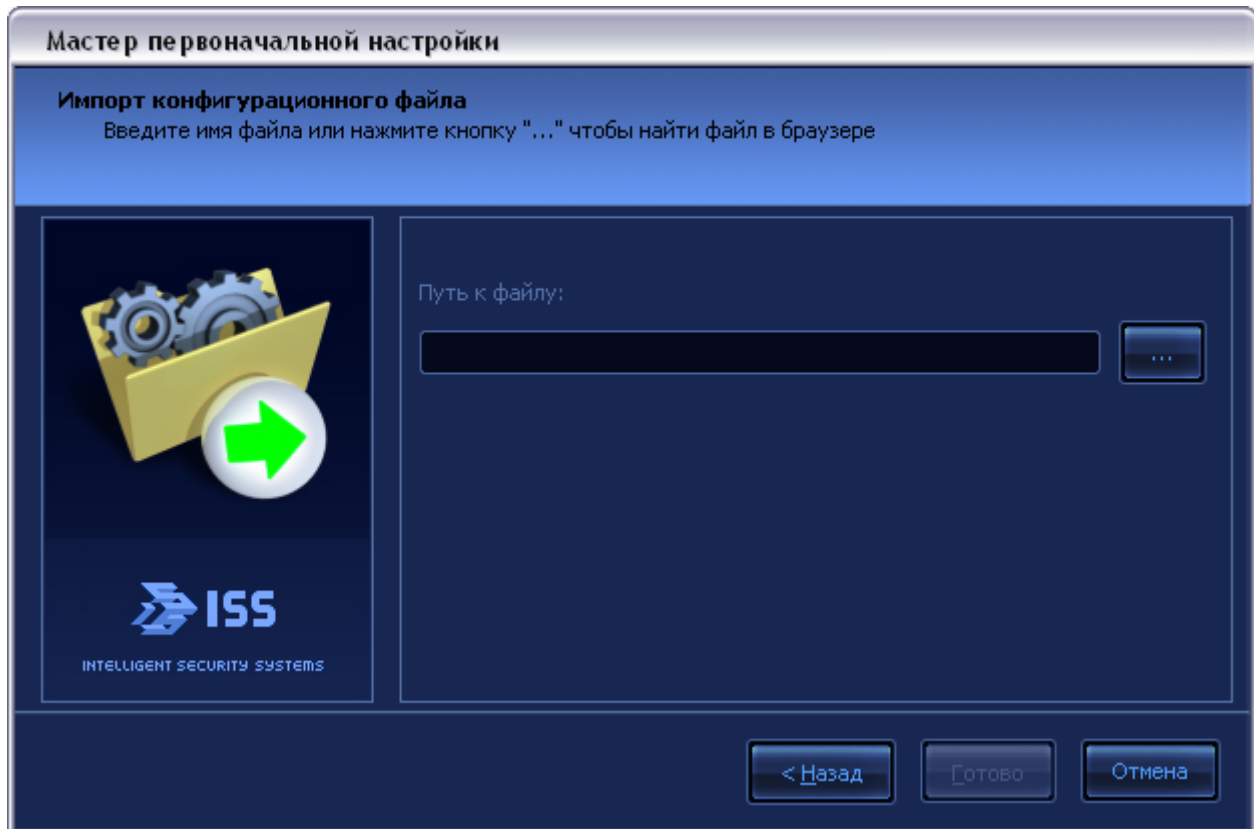


Рис. 29. Мастер первоначальной настройки: импорт файла конфигурации

10. Если выбран тип сценария **Запуск с пустой базой данных**, нажмите кнопку **Готово** для завершения мастера настройки и автоматического запуска системы SecurOS с минимальной конфигурацией, содержащей по одному объекту следующих типов: *Объект охраны*, *Компьютер*, *Экран* и *Монитор* (см. рис. 30).

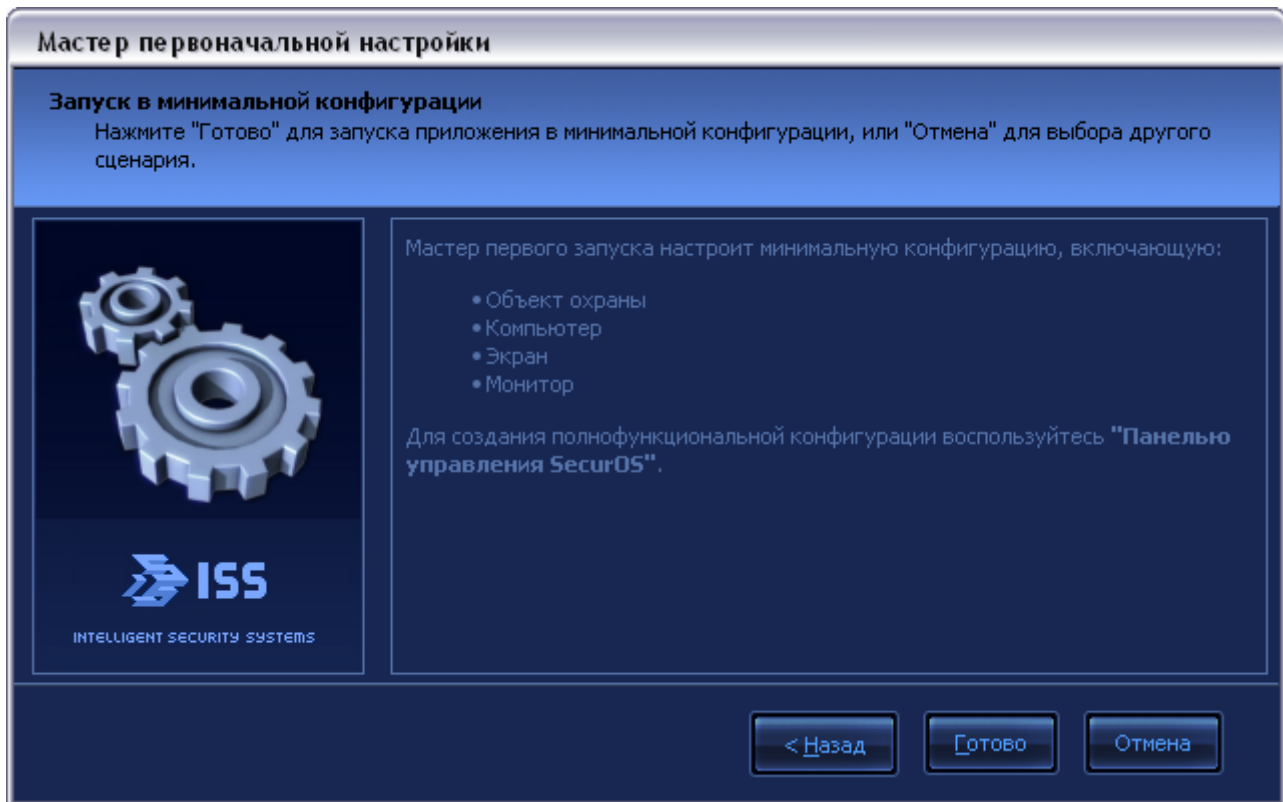


Рис. 30. Мастер первоначальной настройки: создание минимальной конфигурации SecurOS

3.2 Открытие и закрытие панели управления

После завершения инициализации программного обеспечения SecurOS в трее появится значок SecurOS (см. рис. 31).

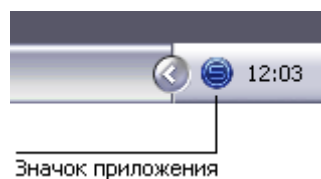


Рис. 31. Пиктограмма SecurOS

Чтобы отобразить панель управления, дважды нажмите значок SecurOS, либо, удерживая клавишу **Ctrl**, подведите курсор мыши в верхнюю часть экрана.

В верхней части монитора появится панель управления SecurOS (см. рис. 32).

Чтобы скрыть панель управления, нажмите кнопку **Скрыть**.



Рис. 32. Панель управления

3.3 Выход из системы

Чтобы выйти из системы SecurOS:

1. Нажмите кнопку **Выполнить** на панели управления.
2. В меню выберите пункт **Завершение работы** (см. рис. 33).

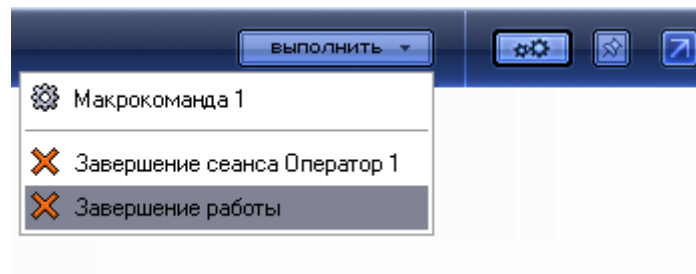


Рис. 33. Выход из системы

Запустится процесс выхода из системы SecurOS, отображаемый в новом окне.

Примечание. Процесс выхода из системы SecurOS, как и процесс входа в систему, может быть ограничен, если это было указано в правах пользователя. По умолчанию при первой установке ограничение отсутствует. Пользователи с ограниченными правами будут иметь возможность только завершить работу с SecurOS (с помощью того же меню), и для выхода из системы потребуется дополнительная идентификация (см. описание настроек уровня доступа в [Руководстве администратора SecurOS](#)).

Приложение 1. Часто задаваемые вопросы

*При запуске Мастера установки появляется диалоговое окно **Обслуживание программ** с возможностью выбора следующих опций: Изменить, Исправить и Удалить. Что это означает?*

Это означает, что программное обеспечение SecurOS уже установлено на этом компьютере или предыдущая версия была удалена некорректно (см. раздел [2.4 Обновление программного обеспечения](#) на стр. 35). Нажмите кнопку **Далее** для продолжения установки программы SecurOS или кнопку **Отмена** для выхода из программы Мастера установки.

Не удается найти файл key.iss на установочном диске / установочный диск потерян. Как получить этот файл?

Обратитесь к системному интегратору или в Службу технической поддержки компании ISS (см. раздел [Обращение за технической поддержкой](#) на стр. 6).

Приложение 1. Часто задаваемые вопросы

При запуске SecurOS появилось сообщение об ошибке. Что делать?

См. таблицу возможных сообщений об ошибке при запуске системы.

Таблица 5. Возможные сообщения об ошибке при запуске системы

Сообщение	Рекомендации
«Ошибка подключения к БД»	Последовательно проведите следующие действия: • Проверьте корректность параметров подключения к БД при помощи утилиты DSAdmin Utility (см. раздел П7.4 Утилита DSAdmin на стр. 94). • Проверьте возможность подключения к БД при помощи утилиты PgAdmin III из комплекта PostgreSQL. • Убедитесь, что служба Windows PostgreSQL Database Server 8.x существует и запущена. • Убедитесь, что пользователь, под которым запущено ПО, имеет права на чтение ключа HKLM/Software/ISS/SecurOS/NISS400/DB в реестре. • Переустановите SecurOS. Обратите особое внимание на разделы установки БД PostgreSQL. • Если перечисленные рекомендации не помогли, обратитесь в Службу технической поддержки. Обязательно приложите к письму информацию о системе, полученную с помощью утилиты ISS System Report (см. раздел П7.2 Утилита ISS System Report на стр. 91).
«Ключ не найден»	Убедитесь, что файл <code>key.iss</code> находится в каталоге, куда было установлено программное обеспечение SecurOS. Если файл отсутствует, то необходимо вручную скопировать его в каталог (файл находится на установочном диске, также его можно получить по электронной почте).
«Ошибка запуска»	Неизвестная ошибка во время запуска системы. Создайте отчет о состоянии системы с помощью утилиты ISS System Report (см. раздел П7.2 Утилита ISS System Report на стр. 91) и обратитесь в Службу технической поддержки для анализа отчета и поиска возможной ошибки (см. раздел Обращение за технической поддержкой на стр. 6).
«Истек срок действия ключа»	Истек срок действия файла <code>key.iss</code>. Обратитесь в Службу технической поддержки для получения нового ключа (см. раздел Обращение за технической поддержкой на стр. 6).

(продолжение на следующей странице)

Приложение 1. Часто задаваемые вопросы

(начало на предыдущей странице)

Сообщение	Рекомендации
«Ключ не поддерживает язык»	При установке SecurOS был выбран язык интерфейса, не соответствующий прописанному в вашем лицензионном ключе. Заново переустановите программное обеспечение SecurOS на этом компьютере и выберите другой язык интерфейса либо приобретите новый файл <code>key.iss</code> , который поддерживает этот язык.
«Ключ не поддерживает страну»	Настройки в главном меню (Пуск → Панель управления → Язык и региональные настройки) отличаются от тех, что прописаны в вашем лицензионном ключе. Проверьте эти настройки либо приобретите новый файл <code>key.iss</code> , который поддерживает текущие настройки.
«Ключ не соответствует плате»	Серийные номера плат видеозахвата TVISSx, установленных на этом компьютере, не соответствуют списку разрешенных плат, прописанных в лицензионном ключе <code>key.iss</code> . Запустите утилиту ISS Hardware Report (см. раздел П7.1 Утилита ISS Hardware Report на стр. 90), чтобы получить отчет по установленным устройствам TVISSx и Guardant, и отправьте отчет Службе технической поддержки для получения соответствующего файла <code>key.iss</code> (см. раздел Обращение за технической поддержкой на стр. 6).

Компьютер не может соединиться с ведущим сервером. Что делать?

- Попробуйте использовать IP-адрес вместо DNS/WINS-имени.
- Удостоверьтесь в правильности указанного IP-адреса.
- Попробуйте уточнить IP-адрес данного компьютера с помощью утилиты `ping` (см. раздел [2.2.6 Соединение компьютеров в единую сеть](#) на стр. 24). Если это не помогло, проверьте настройки брандмауэров на ведущем сервере и на вашем компьютере и откройте доступ к требуемым TCP/IP портам (см. раздел [Приложение 4. Используемые в SecurOS порты](#) на стр. 77).
- Попробуйте с ведущего сервера с помощью утилиты `ping` запросить IP-адрес вашего компьютера. Если это не помогло, проверьте настройки сети и брандмауэров.
- Удостоверьтесь, что в утилите `ipconfig` прописан правильный IP-адрес (см. раздел [2.2.6 Соединение компьютеров в единую сеть](#) на стр. 24) и проверьте корректность регистрации на ведущем сервере.

Внимание! Если компьютер имеет динамический IP-адрес, то при регистрации в сети безопасности SecurOS следует использовать DNS-имя, а не IP-адрес.

Приложение 2. Платы видеозахвата

П2.1 Описание платы TVISS4-02

Плата TVISS4-02 (см. рис. 34) предназначена для захвата четырех каналов в режиме реального времени или до шестнадцати мультимплексных каналов видеостандартов CCIR, PAL и NTSC и восьми моно (четырёх стерео) аудиоканалов.

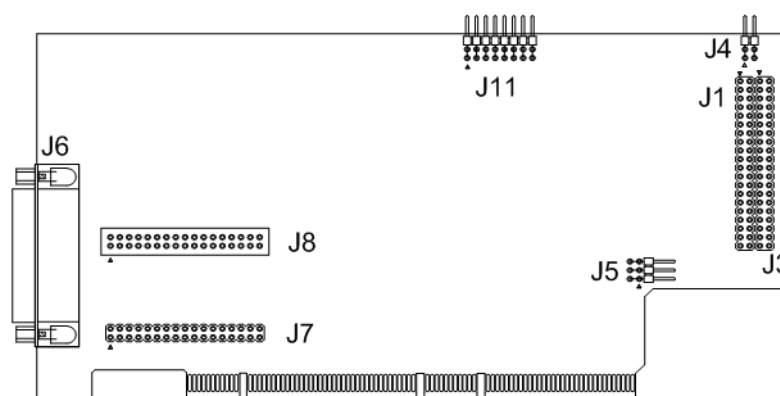


Рис. 34. Плата TVISS4-02

П2.1.1 Подключение платы расширения TVISS4-02EXT

Плата TVISS4-02EXT подключается посредством разъемов **J1**, **J3** и **J8** (см. раздел [П2.3 Описание платы TVISS4-02EXT](#) на стр. 59).

П2.1.2 Подключение видеокамер

Используйте разъем **J6** (см. рис. 35) для подключения видеокоммуникационного кабеля, поставляемого вместе с платой (см. раздел [2.2.2.2 Подключение видеокамер](#) на стр. 21).

Приложение 2. Платы видеозахвата

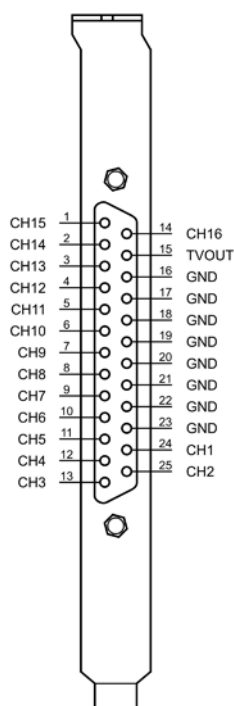


Рис. 35. Вид разъема J6

П2.1.3 Каскадное подключение плат TVISSx-02

Каскадное подключение используется для соединения двух и более плат видеозахвата, образуя один расширенный разъем **J6** (для платы TVISS1-02 используется разъем **J2**, назначение контактов совпадает). Назначения контактов разъемов **J7** и **J6** полностью идентичны. Соединенные таким образом платы будут параллельно получать одни и те же сигналы. При каскадном подключении плат в SecurOS существует возможность настройки определенных микросхем на определенные входные сигналы.

П2.1.4 Подключение аудиовходов

Вид разъема аудиовхода **J11** изображен на рис. 36. Восемь моноканалов могут быть использованы либо раздельно, либо как четыре стереоканала.

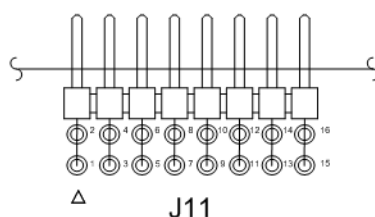


Рис. 36. Вид разъема J11 платы TVISS4-02

Таблица 6. Описание контактов разъема J11

Номер контакта	Название контакта	Описание сигнала
1	Audio IN 1	Вход левого стереоканала 1 / моноканала 1
2	GND	Корпус
3	Audio IN 2	Вход правого стереоканала 1 / моноканала 2
4	GND	Корпус
5	Audio IN 3	Вход левого стереоканала 2 / моноканала 3
6	GND	Корпус
7	Audio IN 4	Вход правого стереоканала 2 / моноканала 4
8	GND	Корпус
9	Audio IN 5	Вход левого стереоканала 3 / моноканала 5
10	GND	Корпус
11	Audio IN 6	Вход правого стереоканала 3 / моноканала 6
12	GND	Корпус
13	Audio IN 7	Вход левого стереоканала 4 / моноканала 7
14	GND	Корпус
15	Audio IN 8	Вход правого стереоканала 4 / моноканала 8
16	GND	Корпус

П2.1.5 Подключение схемы Watchdog

Для подключения схемы Watchdog используется разъем **J4** (см. рис. 37). В нижеприведенной таблице описаны контакты этого разъема. Обратите внимание, что назначение контактов отличается от назначения соответствующих контактов на плате TVISS1-02.

Четыре контакта составляют две пары: **1** и **3**, **2** и **4**. На одну пару контактов подключается шлейф от кнопки **Reset** на передней панели компьютера, а на другую — шлейф, идущий на материнскую плату компьютера, или же к другой плате TVISSx-02, если плата в системе установлена не одна. Таким образом, получается двухпроводная цепь между системной платой, всеми платами видеозахвата TVISSx-02 и кнопкой **Reset**.

Приложение 2. Платы видеозахвата

Внимание! При подключении проводов Watchdog убедитесь в правильной их полярности. Сигнальные провода помечены треугольником и на системных платах, и на платах TVISSx-02.

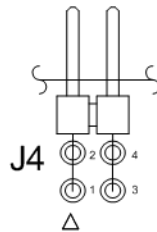


Рис. 37. Вид разъема J4

Таблица 7. Описание контактов разъема J4

Номер контакта	Название контакта	Описание сигнала
1	GND 1	Корпус 1
2	GND 2	Корпус 2
3	Watchdog 1	Сигнал Watchdog 1
4	Watchdog 2	Сигнал Watchdog 2

П2.1.6 Подключение платы расширения TVISS8IO к плате TVISS4-02

Для подключения плат TVISS8IO используется разъем **J5** платы TVISS4-02 (см. рис. 38). При подключении помеченный красным цветом проводник шлейфа платы TVISS8IO должен быть обращен к первому выводу, помеченному треугольником (см. раздел [П2.6 Описание платы TVISS8IO](#) на стр. 67).

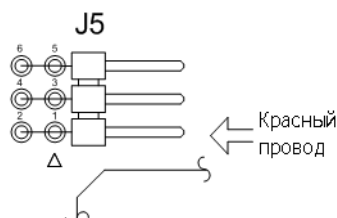


Рис. 38. Вид разъема J5

П2.2 Описание платы TVISS1-02

Плата TVISS1-02 (см. рис. 39) предназначена для захвата одного канала в режиме реального времени или до шестнадцати мультиплексных каналов видеостандартов CCIR, PAL и NTSC и двух моно (одного стерео) аудиоканалов.

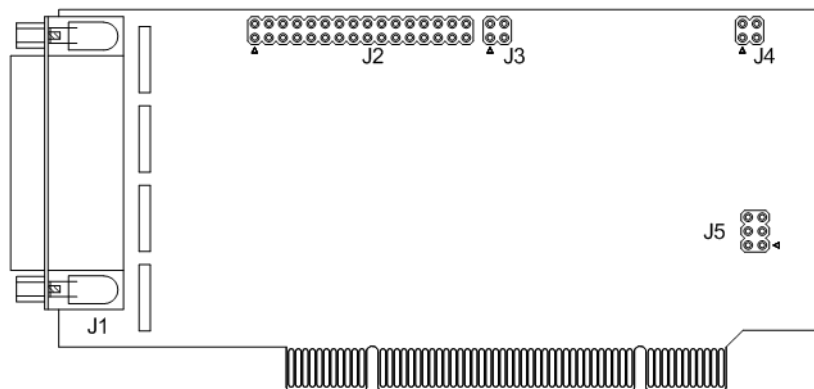


Рис. 39. Плата TVISS1-02

П2.2.1 Подключение видеокамер

Используйте разъем **J1** для подключения видеокоммуникационного кабеля, поставляемого вместе с платой (см. раздел 2.2.2.2 Подключение видеокамер на стр. 21). Разъем аналогичен показанному на рис. 35.

П2.2.2 Каскадное подключение плат TVISSx-02

Каскадное подключение используется для соединения двух и более плат видеозахвата, образуя один расширенный разъем **J2** (для платы TVISS4-02 используется разъем **J6**, назначение контактов совпадает). Назначения контактов разъемов **J2** и **J1** полностью идентичны. Соединенные таким образом платы будут параллельно получать одни и те же сигналы. При каскадном подключении плат в SecurOS существует возможность настройки определенных микросхем на определенные входные сигналы.

П2.2.3 Подключение аудиовходов

Вид разъема аудиовхода **J3** изображен на рис. 40. Два моноканала могут быть использованы либо раздельно, либо как один стереоканал.

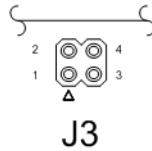


Рис. 40. Вид разъема J3

Таблица 8. Описание контактов разъема J3

Номер контакта	Название контакта	Описание сигнала
1	GND	Корпус
2	Audio IN 1	Вход правого стереоканала 1/моноканала 1
3	GND	Корпус
4	Audio IN 2	Вход левого стереоканала 1/моноканала 2

П2.2.4 Подключение схемы Watchdog

Для подключения схемы Watchdog используется разъем **J4** (см. рис. 41). В нижеприведенной таблице описаны контакты этого разъема. Обратите внимание, что назначение контактов отличается от назначения соответствующих контактов на плате TVISS1-02.

Четыре контакта составляют две пары: **1** и **2**, **3** и **4**. На одну пару контактов подключается шлейф от кнопки **Reset** на передней панели компьютера, а на другую — шлейф, идущий на материнскую плату компьютера, или же к другой плате TVISSx-02, если плата в системе установлена не одна. Таким образом, получается двухпроводная цепь между системной платой, всеми платами видеозахвата TVISSx-02 и кнопкой **Reset**.

Внимание! При подключении проводов Watchdog убедитесь в правильной их полярности. Сигнальные провода помечены треугольником и на системных платах, и на платах TVISSx-02.

Приложение 2. Платы видеозахвата

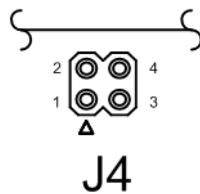


Рис. 41. Схема разъема J4

Таблица 9. Описание контактов разъема J4

Номер контакта	Название контакта	Описание сигнала
1	Watchdog 1	Сигнал Watchdog 1
2	GND 1	Корпус 1
3	Watchdog 2	Сигнал Watchdog 2
4	GND 2	Корпус 2

П2.2.5 Подключение платы расширения TVISS8IO к плате TVISS1-02

Для подключения плат TVISS8IO используется разъем **J5** (см. рис. 42). При подключении помеченный красным цветом проводник шлейфа платы TVISS8IO должен быть обращен к первому выводу, помеченному треугольником (см. раздел [П2.6 Описание платы TVISS8IO](#) на стр. 67).

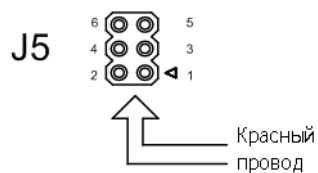


Рис. 42. Подключение платы TVISS8IO

П2.3 Описание платы TVISS4-02EXT

Плата TVISS4-02EXT (см. рис. 43) была разработана как расширение платы TVISS4-02: для захвата четырех дополнительных каналов видеостандартов CCIR, PAL или NTSC в режиме реального времени и дополнительно восьми моно (четырёх стерео) аудиоканалов.

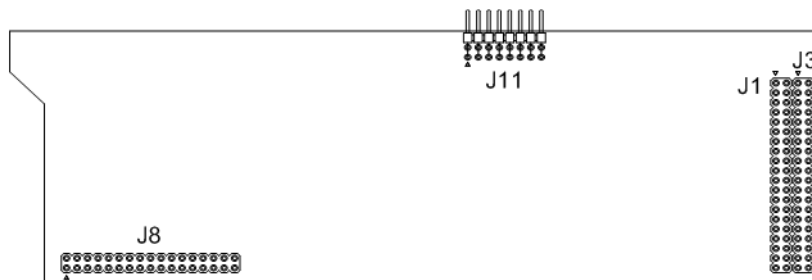


Рис. 43. Плата TVISS4-02EXT

П2.3.1 Подключение платы TVISS4-02

Плата TVISS4-02EXT подключается к плате TVISS4-02 через разъемы **J1**, **J3** и **J8** (см. раздел [П2.1 Описание платы TVISS4-02](#) на стр. 52).

П2.3.2 Подключение аудиовходов

Назначение контактов аудиовхода (**J11**) аналогично назначению контактов платы TVISS4-02 (см. раздел [П2.3.2 Подключение аудиовходов](#) на стр. 59).

П2.4 Описание плат TVISS4E и TVISS8E

Платы TVISS4E и TVISS8E рассчитаны на шину PCI Express.

Плата TVISS4E (см. рис. 44) предназначена для захвата четырех каналов в режиме реального времени или до шестнадцати мультиплексных каналов видеостандартов CCIR, PAL и NTSC и четырех моно (двух стерео) аудиоканалов.

Плата TVISS8E (см. рис. 45) представляет собой ту же плату TVISS4E с подключенной дочерней платой и предназначена для захвата восьми каналов в режиме реального времени или до шестнадцати мультиплексных каналов видеостандартов CCIR, PAL и NTSC и восьми моно (четырёх стерео) аудиоканалов.

Приложение 2. Платы видеозахвата

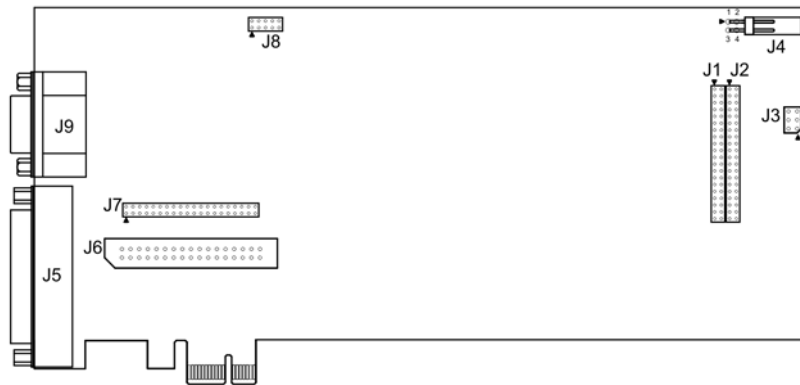


Рис. 44. Плата TVISS4E



Рис. 45. Плата TVISS8E

П2.4.1 Подключение видеокамер

Используйте разъем **J5** для подключения видеокоммуникационного кабеля, поставляемого вместе с платой (см. раздел [2.2.2.2 Подключение видеокамер](#) на стр. 21). Вид аудио- и видеоразъемов показан на рис. 46.

П2.4.2 Подключение аудиовходов

Вид разъема аудиовхода (**J9**) изображен на рис. 46. Восемь моноканалов могут быть использованы либо раздельно, либо как четыре стереоканала.

Приложение 2. Платы видеозахвата

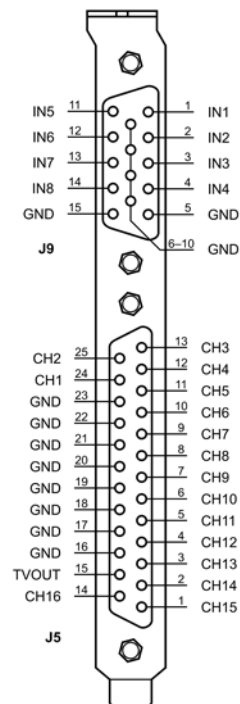


Рис. 46. Вид разъема J9 (аудио) и J5 (видео)

Таблица 10. Описание контактов разъема J9

Номер контакта	Название контакта	Описание сигнала
1	Audio IN 1	Вход левого стереоканала 1 / моноканала 1
2	Audio IN 2	Вход правого стереоканала 1 / моноканала 2
3	Audio IN 3	Вход левого стереоканала 2 / моноканала 3
4	Audio IN 4	Вход правого стереоканала 2 / моноканала 4
5	GND	Корпус
6	GND	Корпус
7	GND	Корпус
8	GND	Корпус
9	GND	Корпус
10	GND	Корпус
11	Audio IN 5	Вход левого стереоканала 3 / моноканала 5
12	Audio IN 6	Вход правого стереоканала 3 / моноканала 6

(продолжение на следующей странице)

Приложение 2. Платы видеозахвата

(начало на предыдущей странице)

Номер контакта	Название контакта	Описание сигнала
13	Audio IN 7	Вход левого стереоканала 4 / моноканала 7
14	Audio IN 8	Вход правого стереоканала 4 / моноканала 8
15	GND	Корпус

П2.4.3 Каскадное подключение плат TVISSxE

Каскадное подключение используется для соединения двух и более плат видеозахвата TVISSxE, образуя один расширенный разъем **J6**. Соединенные таким образом платы будут параллельно получать одни и те же сигналы. При каскадном подключении плат в SecurOS существует возможность настройки определенных микросхем на определенные входные сигналы.

П2.4.4 Подключение схемы Watchdog

Для подключения схемы Watchdog используется разъем **J4** (см. рис. 47). В нижеприведенной таблице описаны контакты этого разъема. Обратите внимание, что назначение контактов отличается от назначения соответствующих контактов на плате TVISS1-02.

Четыре контакта составляют две пары: **1** и **3**, **2** и **4**. На одну пару контактов подключается шлейф от кнопки **Reset** на передней панели компьютера, а на другую — шлейф, идущий на материнскую плату компьютера, или же к другой плате TVISS, если плата в системе установлена не одна. Таким образом, получается двухпроводная цепь между системной платой, всеми платами видеозахвата TVISS и кнопкой **Reset**.

Внимание! При подключении проводов Watchdog убедитесь в правильной их полярности. Сигнальные провода помечены треугольником и на системных платах, и на платах TVISS.

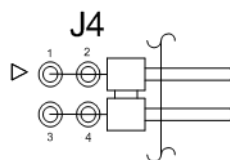


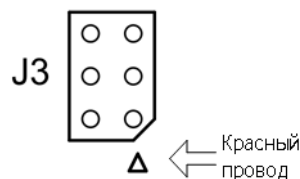
Рис. 47. Вид разъема J4

Таблица 11. Описание контактов разъема J4

Номер контакта	Название контакта	Описание сигнала
1	GND 1	Корпус 1
2	GND 2	Корпус 2
3	Watchdog 1	Сигнал Watchdog 1
4	Watchdog 2	Сигнал Watchdog 2

П2.4.5 Подключение платы расширения TVISS8IO к плате TVISS4E (TVISS8E)

Для подключения плат TVISS8IO используется разъем **J3** (см. рис. 48). При подключении помеченный красным цветом проводник шлейфа платы TVISS8IO должен быть обращен к первому выводу, помеченному треугольником (см. раздел [П2.6 Описание платы TVISS8IO](#) на стр. 67).

**Рис. 48.** Вид разъема J3

П2.5 Описание плат TVISS PCI-E8 R1 и TVISS A8 R1

Плата TVISS PCI-E8 R1 рассчитана на шину PCI Express. Плата расширения TVISS A8 R1 (плата аудио модуля) устанавливается непосредственно на плату TVISS PCI-E8 R1 (см. раздел [П2.5.4 Подключение платы расширения TVISS A8 R1 к плате TVISS PCI-E8 R1](#) на стр. 65).

Плата TVISS PCI-E8 R1 (см. рис. 49) предназначена для захвата шестнадцати каналов в режиме реального времени или до шестнадцати мультимплексных каналов видеостандартов CCIR, PAL и NTSC и восьми моно (четырех стерео) аудиоканалов, а также организации управления до шести плат расширения TVISS8IO.

Приложение 2. Платы видеозахвата

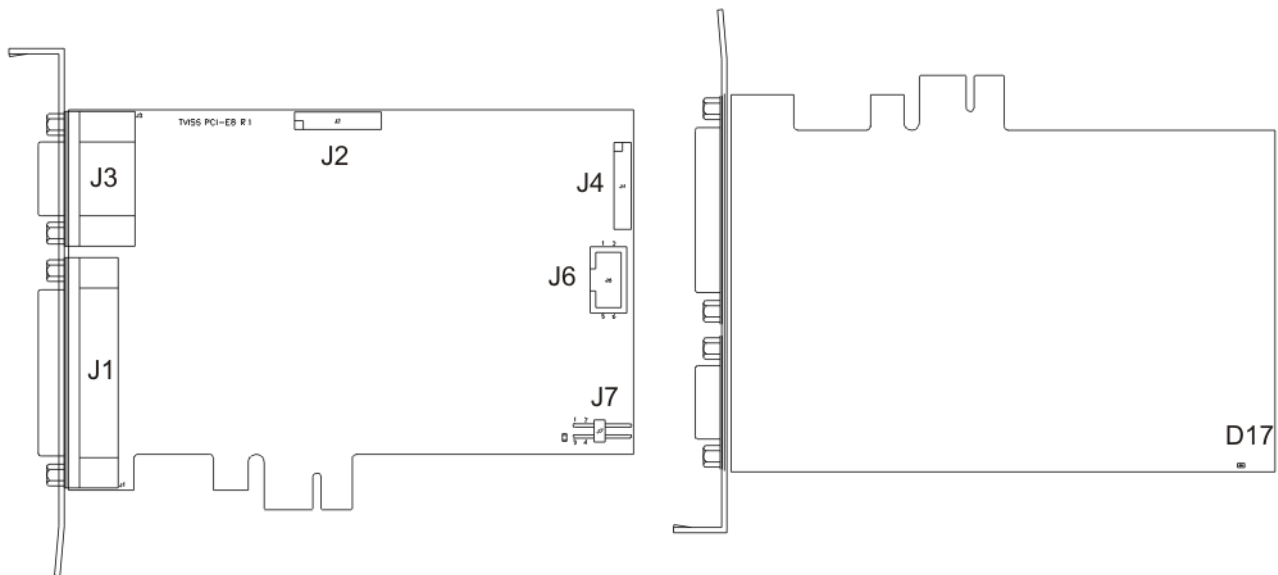


Рис. 49. Плата TVISS PCI-E8 R1: лицевая (слева) и оборотная (справа) стороны

Плата расширения TVISS A8 R1 (см. рис. 50) предназначена для оцифровки до 8 аудиоканалов, интегрированных на плате TVISS PCI-E8 R1.



Рис. 50. Плата расширения TVISS A8 R1

П2.5.1 Подключение видеокамер

Используйте разъем **J1** для подключения видеокоммуникационного кабеля, поставляемого вместе с платой (см. раздел [2.2.2.2 Подключение видеокамер](#) на стр. 21). Вид аудио- и видеоразъемов аналогичен виду для плат TVISSxE (см. раздел [П2.4.1 Подключение видеокамер](#) на стр. 60; разъемы **J1** и **J3** на плате TVISS PCI-E8 R1 соответствуют разъемам **J5** и **J9** на платах TVISSxE).

П2.5.2 Подключение аудиовходов

Разъем аудиовхода (**J3**) аналогичен разъему **J9** на платах TVISSxE (см. раздел [П2.4.2 Подключение аудиовходов](#) на стр. 60). Восемь моноканалов могут быть использованы либо отдельно, либо как четыре стереоканала.

П2.5.3 Подключение схемы Watchdog

Для подключения схемы Watchdog используется разъем **J7**, аналогичный разъему **J4** на платах TVISSxE (см. рис. 47). В нижеприведенной таблице описаны контакты этого разъема. Обратите внимание, что назначение контактов отличается от назначения соответствующих контактов на платах TVISSxE.

Четыре контакта составляют две пары: **1** и **2**, **3** и **4**. На одну пару контактов подключается шлейф от кнопки **Reset** на передней панели компьютера, а на другую — шлейф, идущий на материнскую плату компьютера, или же к другой плате TVISS, если плата в системе установлена не одна. Таким образом, получается двухпроводная цепь между системной платой, всеми платами видеозахвата TVISS и кнопкой **Reset**.

Внимание! При подключении проводов Watchdog убедитесь в правильной их полярности. Сигнальные провода помечены треугольником и на системных платах, и на платах TVISS.

Таблица 12. Описание контактов разъема J4

Номер контакта	Название контакта	Описание сигнала
1	GND 1	Корпус 1
2	Watchdog 1	Сигнал Watchdog 1
3	GND 2	Корпус 2
4	Watchdog 2	Сигнал Watchdog 2

П2.5.4 Подключение платы расширения TVISS A8 R1 к плате TVISS PCI-E8 R1

Плата расширения TVISS A8 R1 (модуль оцифровки аудио) подключается при необходимости оцифровки захваченного аудиосигнала непосредственно на плате TVISS PCI-E8 R1. Плата подключается через разъемы **J2** и **J4** (см. рис. 49 и 50).

П2.5.5 Подключение платы расширения TVISS8IO к плате TVISS PCI-E8 R1

Для подключения плат TVISS8IO используется разъем **J6**, соответствующий разъему **J3** на платах TVISSxE (см. рис. 48). Процедура подключения аналогична подключению к платам TVISSxE (см. раздел П2.4.5 Подключение платы расширения TVISS8IO к плате TVISS4E (TVISS8E) на стр. 63).

Примечание. Плата TVISS PCI-E8 R1 допускает каскадное подключение до шести плат расширения TVISS8IO (см. раздел П2.6.3 Каскадное подключение плат TVISS8IO на стр. 68).

П2.5.6 Индикация состояния

Используйте светодиод **D17** для проверки состояния оборудования (см. рис. 49 и 50).

Значения возможных состояний светодиода **D17** для платы TVISS8E-R1:

- Мигание с частотой 1 раз в секунду — драйвер платы установлен, плата функционирует нормально, сторожевой таймер отключен;
- Мигание с частотой 4 раза в секунду — драйвер платы установлен, плата функционирует нормально, сторожевой таймер включен;
- Не горит или непрерывно светится — драйвер платы не установлен или плата неисправна.

Мигание светодиода **D17** на плате TVISS A8 R1 сигнализирует о частоте оцифровки аудио сигналов (см. таблицу ниже). Светодиод погашен, если аудиоподсистема не была инициализирована.

Таблица 13. Соответствие частоты мигания светодиода и частоты оцифровки аудио сигналов

Частота оцифровки аудио, кГц	Частота мигания светодиода, в секунду
6	0.75
8	1
16	2
32	4
48 (значение по умолчанию)	6
64	8
96	12

П2.6 Описание платы TVISS8IO

Плата TVISS8IO (см. рис. 51) спроектирована для управления до восьми изолированных входов (петли безопасности) и выходов (реле).

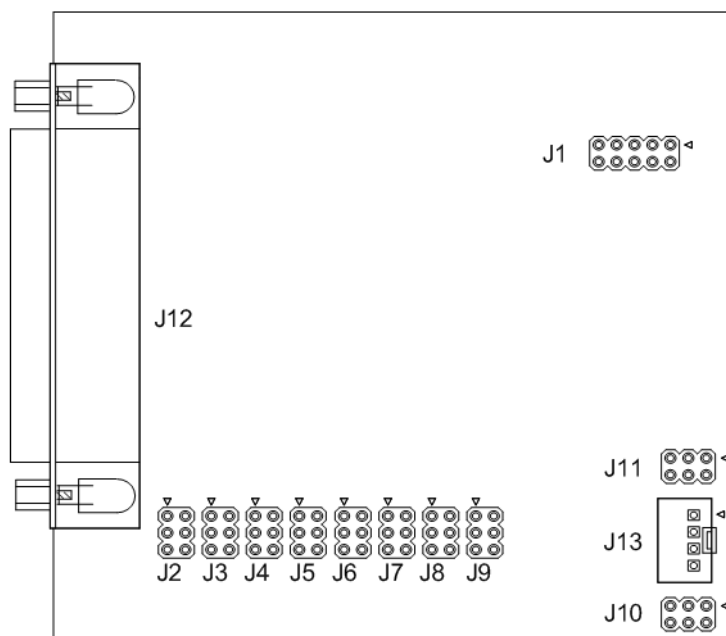


Рис. 51. Плата TVISS8IO

П2.6.1 Подключение питания

Для подключения питания к плате TVISS8IO используется разъем **J13** (см. рис. 52), который представляет собой стандартный разъем для питания флоппи-дисководов.

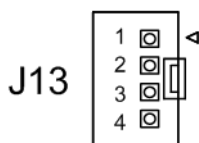


Рис. 52. Вид разъема J13

Таблица 14. Описание контактов разъема J13

Номер контакта	Название контакта	Описание сигнала
1	+5 V	Питание +5 В

(продолжение на следующей странице)

Приложение 2. Платы видеозахвата

(начало на предыдущей странице)

Номер контакта	Название контакта	Описание сигнала
2	GND	Корпус
3	GND	Корпус
4	—	Не используется

П2.6.2 Подключение платы TVISS8IO к TVISSx-02 и TVISSxE

Для подключения к платам TVISSx-02 и TVISSxE используется разъем **J10** (см. рис. 53). В комплекте с TVISS8IO поставляется шлейф для подключения. При подключении этот шлейф должен быть обращен проводником, помеченным красным цветом, в сторону первого вывода, помеченного треугольником. Аналогичным способом подключается другой конец шлейфа к плате TVISSx-02 или TVISSxE.

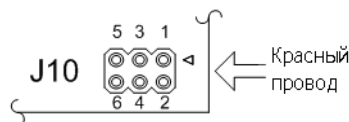


Рис. 53. Вид разъема J10

П2.6.3 Каскадное подключение плат TVISS8IO

Две (и более) платы TVISS8IO могут быть подключены каскадно (см. рис. 54), то есть вторая (и каждая последующая) плата подключается непосредственно к первой (или предыдущей) TVISS8IO так же, как и первая к TVISSx-02 (или TVISSxE). Для этих целей используется разъем **J11** (см. рис. 55) и тот же шлейф, поставляемый в комплекте.

П2.6.4 Настройка цифровых входов и выходов

Каждый вход имеет две ступени срабатывания. Первая ступень срабатывает при токе ~ 3 мА (срабатывание при 3,2 мА, отпускание при 2,8 мА), вторая ступень срабатывает при токе $\sim 4,2$ мА (срабатывание при 4,4 мА, отпускание при 4,0 мА). Нормальное состояние охранного шлейфа — когда первая ступень сработала, а вторая еще нет. Для этого через шлейф должен протекать ток 3,6 мА. На плате установлен источник питания 24 В, который через два резистора (согласующий и постоянный), служит источником тока для охранных шлейфов. Эти резисторы рассчитаны на шлейф с сопротивлением 3 кОм.

Приложение 2. Платы видеозахвата

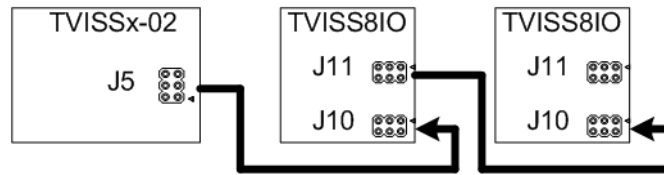


Рис. 54. Каскадная схема подключения

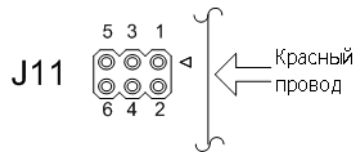


Рис. 55. Вид разъема J11

Плата TVISS8IO имеет восемь цифровых входов. Внутренний источник тока подключается, когда замыкаем выводы **1–3** и **2–4** перемычек **J2–J9**. Если поставить перемычки так, чтобы замкнут выводы **3–5** и **4–6** (см. рис. 56), то к выводам **INPx** и **INN_x** будут подключены неполярные датчики тока, к которым можно подключить контакты охранных шлейфов.

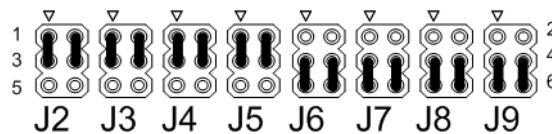


Рис. 56. Вид джамперов J2–J9

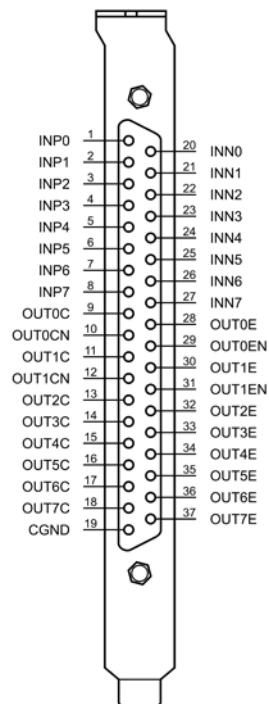
Выводы **INN_x** и **INPx** (см. рис. 57) могут использоваться в любой полярности.

Плата TVISS8IO имеет восемь управляющих выходов (**OUT0–OUT7**). Выходы **OUT0** и **OUT1** имеют как нормально замкнутые контакты, так и нормально разомкнутые. Остальные выходы имеют только нормально разомкнутые контакты. Выходы **OUT0** и **OUT1** можно использовать для создания знакопеременного источника питания.

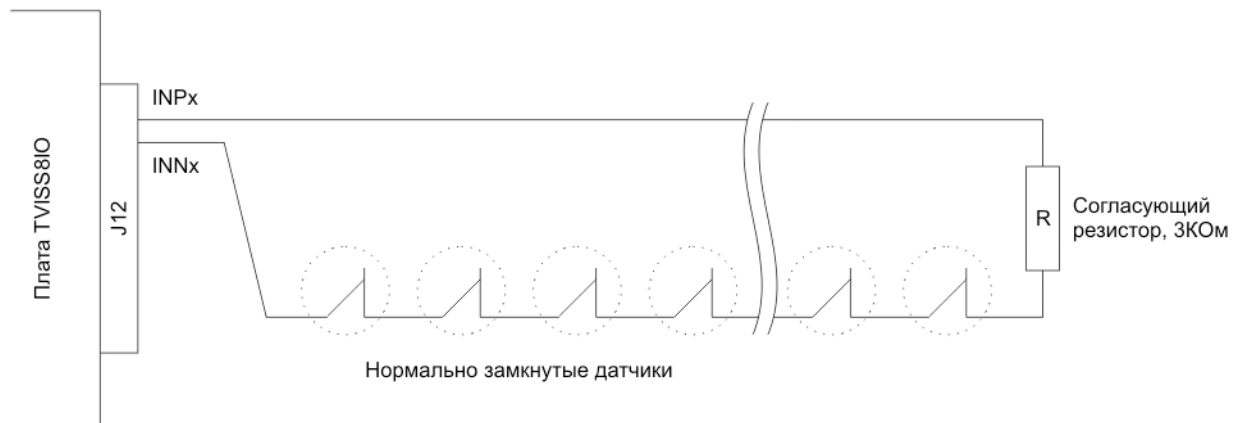
Каждый выход может управлять током до 50 мА при напряжении до 35 В. Выходы обозначены следующим образом:

- **OUTxC** — коллектор нормально разомкнутого выхода;
- **OUTxE** — эмиттер нормально разомкнутого выхода;
- **OUTxCN** — коллектор нормально замкнутого выхода;
- **OUTxEN** — эмиттер нормально замкнутого выхода.

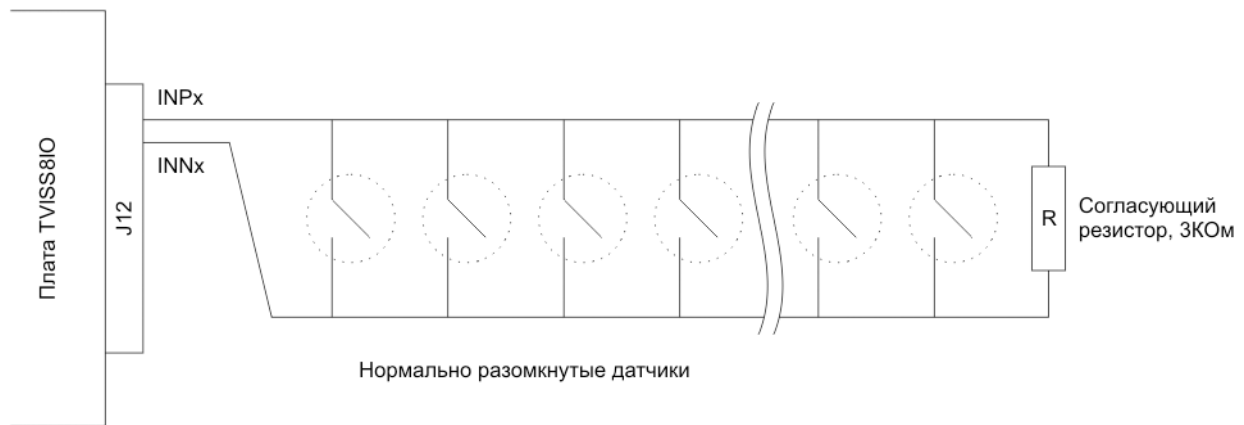
Приложение 2. Платы видеозахвата

**Рис. 57.** Вид разъема J12

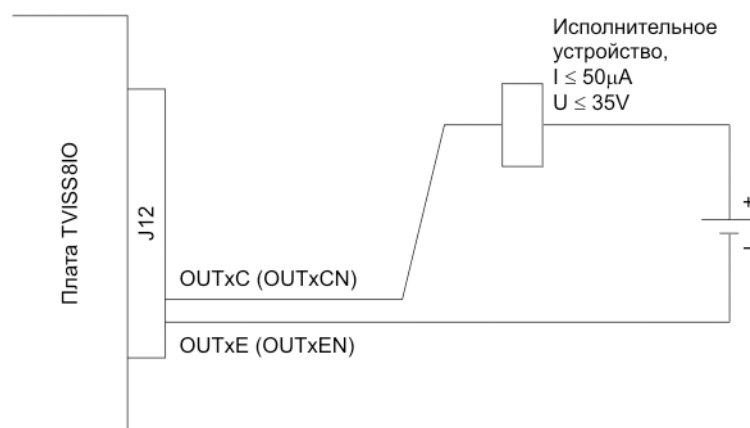
На рис. 58 и 59 приведены схемы подключения лучей с нормально замкнутыми и нормально разомкнутыми контактами.

**Рис. 58.** Луч с типом срабатывания на размыкание

Приложение 2. Платы видеозахвата

**Рис. 59.** Луч с типом срабатывания на замыкание

На рис. 60 приведена схема подключения исполнительного устройства к плате TVISS8IO. Если требуется большее напряжение или больший ток, то при необходимости используйте определенный гальванический разделитель или оптическую развязку.

**Рис. 60.** Схема подключения исполнительного устройства

Приложение 3. Технические данные

П3.1 Разрешение изображения

В таблице 15 представлены разрешения изображений в SecurOS.

Таблица 15. Разрешение изображения

Установленное значение	Разрешение, pix (PAL)	Разрешение, pix (NTSC)
Нормальное (CIF1)	352 × 288	320 × 240
Высокое (CIF2)	704 × 288	640 × 240
Полное (CIF4)	704 × 576	640 × 480

П3.2 Рекомендуемые процессоры для видеосерверов

Таблица 16. Процессоры

Общая скорость передачи кадров	Рекомендуемые процессоры
100	AMD Athlon-64 3800+ Intel Pentium E2140 Dual Core 1.6 GHz/1MB cache/800MHz Intel Pentium IV 3.0 GHz/2MB cache/800MHz
200	AMD Athlon-64 X2 5600+ 2MB cache/1000 MHz Intel Core 2 Duo E6400 2.13 GHz/2MB cache/1066 MHz Intel Core 2 Duo E6420 2.13 GHz/4MB cache/1066 MHz

(продолжение на следующей странице)

Приложение 3. Технические данные

(начало на предыдущей странице)

Общая скорость передачи кадров	Рекомендуемые процессоры
400	Два процессора 2 × AMD Opteron 2.6 GHz Два процессора 2 × Intel Xeon 2.0 GHz

П3.3 Скорость передачи данных

В таблице 17 представлены данные для платы TVISS4-02 (см. раздел П2.1 Описание платы TVISS4-02 на стр. 52).

Таблица 17. Скорость платы TVISS4-02 (общее количество кадров в секунду)

TVISS4	PAL (4 камеры)	NTSC (4 камеры)
Максимальная	100	120
Средняя	50	60
Минимальная	50	60

В таблице 18 представлены данные для платы TVISS1-02 (см. раздел П2.2 Описание платы TVISS1-02 на стр. 56).

Таблица 18. Скорость платы TVISS1-02 (общее количество кадров в секунду)

TVISS1	Подключена одна камера		Подключено несколько камер	
Максимальная	25	30	17	20
Средняя	12.5	15	17	20
Минимальная	6.25	10	15	17

П3.4 Размер видеокadra

В нижеследующих таблицах приведены значения объема записываемого на диск кадра (Кбайт) в зависимости от величины установленного разрешения, компрессии и цветности. Таблицы структурированы по типу видеосигнала (PAL/NTSC) и сложности изображения. К «простому» изображению относится статическое изображение (например, изображение с камер, установленных в коридоре или других комнатах, в которых наблюдается низкая интенсивность движения). Под «комплексным» изображением понимается динамическая картинка (например, многолюдная территория, движение транспорта).

Таблица 19. Размер кадра (Кбайт) для простого изображения, PAL

Разрешение и цветность изображения	Уровень компрессии (0/1/2/3/4/5)					
	0	1	2	3	4	5
CIF1 (352 × 288) ч/б	99	18	5	4	3	3
CIF2 (704 × 288) ч/б	198	29	8	8	4	3
CIF4 (704 × 576) ч/б	396	49	13	13	7	5
CIF1 (352 × 288) цв.	148	25	7	7	4	4
CIF2 (704 × 288) цв.	297	40	11	11	5	5
CIF4 (704 × 576) цв.	594	61	16	16	9	8

Таблица 20. Размер кадра (Кбайт) для простого изображения, NTSC

Разрешение и цветность изображения	Уровень компрессии (0/1/2/3/4/5)					
	0	1	2	3	4	5
CIF1 (320 × 240) ч/б	75	14	4	3	2	2
CIF2 (640 × 240) ч/б	150	22	6	6	3	2
CIF4 (640 × 480) ч/б	300	37	10	10	5	4
CIF1 (320 × 240) цв.	112	19	5	5	3	3
CIF2 (640 × 240) цв.	225	30	8	8	4	4
CIF4 (640 × 480) цв.	450	46	12	12	7	6

Приложение 3. Технические данные

Таблица 21. Размер кадра (Кбайт) для комплексного изображения, PAL

Разрешение и цветность изображения	Уровень компрессии (0/1/2/3/4/5)					
	0	1	2	3	4	5
CIF1 (320 × 240) ч/б	75	33	3	3	4	5
CIF2 (640 × 240) ч/б	150	59	5	5	5	5
CIF4 (640 × 480) ч/б	300	97	11	11	9	8
CIF1 (320 × 240) цв.	112	39	5	5	5	5
CIF2 (640 × 240) цв.	225	68	10	10	5	5
CIF4 (640 × 480) цв.	450	114	17	17	11	10

Таблица 22. Размер кадра (Кбайт) для комплексного изображения, NTSC

Разрешение и цветность изображения	Уровень компрессии (0/1/2/3/4/5)					
	0	1	2	3	4	5
CIF1 (320 × 240) ч/б	75	33	3	3	4	4
CIF2 (640 × 240) ч/б	150	59	5	5	5	5
CIF4 (640 × 480) ч/б	300	97	11	11	9	8
CIF1 (320 × 240) цв.	112	39	5	5	5	5
CIF2 (640 × 240) цв.	225	68	10	10	5	5
CIF4 (640 × 480) цв.	450	114	17	17	11	10

П3.5 Время хранения видеоархива / объем жесткого диска

В нижеследующих таблицах приведены значения времени хранения видеоархива (сутки) в зависимости от размеров видеокadra (Кбайт) и указанного объема жесткого диска. Данные приведены для одиночной камеры. Если на сервер приходится несколько камер, необходимо скорректировать данные (числа в таблице разделить на количество камер).

Приложение 3. Технические данные

Таблица 23. Время хранения видеоархива при круглосуточной ежедневной записи

Средний размер кадра (Кбайт)	Объем диска (150/200/250/300 ГБ)			
2	73	97	122	146
4	37	49	61	73
8	18	24	31	37
16	9	12	15	18
32	4.5	6	7.5	9
64	2.2	3	3.8	4.5

Таблица 24. Время хранения видеоархива (запись по детектору)

Средний размер кадра (Кбайт)	Объем диска (150/200/250/300 ГБ)			
2	291	388	485	582
4	146	194	243	291
8	73	97	121	146
16	36	49	61	73
32	18	24	30	36
64	9	12	15	18

Приложение 4. Используемые в SecurOS порты

SecurOS и подключаемые модули для взаимодействия используют ряд портов TCP/IP. Проверьте настройки брандмауэра и откройте для исполнимых файлов SecurOS (*.exe), расположенных в корневом каталоге SecurOS, следующие порты в оба направления:

Таблица 25. Порты TCP/IP

Модуль	Номер порта
Основная подсистема	
Соединение с основной подсистемой	21111 (для установки SecurOS необходимо предварительно открыть этот порт)
Модули основной подсистемы	
Графическая карта	21051
Протокол событий системы	21055
Программируемая клавиатура	21005
Интерфейс IIDK	21030
Видеоподсистема	
Видеомонитор, видеоконцентратор, устройство видеозахвата, видеокамеры	21050
Поворотное устройство	21010
Поток живого видео	20900
Поток видеоконцентратора	20902
Конвертер Архива	22131
Диалог Конвертера Архива	22138
Аудиоподсистема	
Микрофон	21004
Аудиопоток	20910
Аудиопроигрыватель	21060

(продолжение на следующей странице)

Приложение 4. Используемые в SecurOS порты

(начало на предыдущей странице)

Модуль	Номер порта
Охранно-пожарная подсистема	
Луч, Реле	21003
Подсистема оповещения	
Служба коротких сообщений	22092
Электронная почта	22093
Служба голосового оповещения	22094
Подсистема контроля доступа	
Служба контроля доступа	21057
Модуль распознавания номеров автомобилей	
Детектор камеры	21033
Детектор устройства	21081
Пользовательский интерфейс оператора	21062 (21091)
Внешняя база данных	22100
Модуль распознавания номеров железнодорожных вагонов	
Сервер (Pro)	22120
Сервер (Light)	21121
Детектор камеры	21122
Модуль распознавания лиц	
Устройство	21080
Поток фотоданных	20920
Пользовательский интерфейс оператора	21061
Модуль анализа движения	
Устройство	22110
Устройство (Pro)	22111
Модуль POS	
POS Терминал	22110

(продолжение на следующей странице)

Приложение 4. Используемые в SecurOS порты

(начало на предыдущей странице)

Модуль	Номер порта
Устройство ложного детектирования	22111
Подсистемы подключения устройств сторонних производителей	
«Vista»	21015
«Рубеж»	21002
«Flex»	21043
«Apollo»	21014
«Болид»	21025

Приложение 5. Установка аппаратного обеспечения сторонних производителей

Для моделей, не указанных в этом разделе, используйте описания их производителей.

П5.1 Подключение купольной камеры Panasonic WV-CS850

Для подключения купольной камеры Panasonic WV-CS850 по протоколу RS485 используется разъем **RJ11** (см. рис. 61).

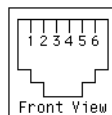


Рис. 61. Вид разъема RJ11

Таблица 26. Описание разъема RJ11

Разъем RJ11	Сигнал
1	Аппаратное управление исходящим потоком (опционален)
2	Выход (T+)
3	Выход заземления (T–)
4	Вход заземления (R–)
5	Вход (R+)
6	Аппаратное управление входящим потоком (опционален)

Приложение 5. Установка аппаратного обеспечения сторонних производителей

Для работы камеры Panasonic WV-CS850 в полнодуплексном режиме используйте следующую схему подключения конвертера RS485-RS232:

Таблица 27. Сигналы IC485

IC485	Шина данных камеры
1	Выход/вход
2	Выход заземления/вход заземления
3	Не используется
4	Не используется

П5.2 Подключение купольных камер к видеосерверу Bosch VIP X1

При подключении камеры с поворотным устройством к сети SecurOS через видеосервер **Bosch VIP X1** укажите следующие параметры в настройках соответствующего объекта *PTZ-контроллер* (см. [Руководство администратора SecurOS](#)):

- **Протокол телеметрии** — выберите один из PTZ-протоколов, поддерживаемых видеосервером **Bosch VIP X1** (см. ниже таблицу 28 соответствий значений в списке и PTZ-протоколов);

Внимание! Выбранный протокол должен соответствовать протоколу, указанному в собственных настройках видеосервера **Bosch VIP X1** (см. рис. 62, поле **Serial port function**).

- **DTR, RTS** — при подключении поворотного устройства по интерфейсу RS485 активируйте оба поля;
- **Использовать удаленное устройство** — активируйте поле и выберите из списка объект *Устройство видеозахвата*, соответствующий видеосерверу **Bosch VIP X1**.

Внимание! Идентификатор дочернего объекта *Поворотное устройство* должен быть равен идентификатору аналоговой камеры, указанному в собственных настройках видеосервера (см. рис. 62, поле **Camera ID**), при подключении камеры к серверу через последовательный порт.

Приложение 5. Установка аппаратного обеспечения сторонних производителей



Рис. 62. Определение протокола и идентификатора камеры в настройках видеосервера **Bosch VIP X1**

Таблица 28. Поддерживаемые PTZ-протоколы (устройство **Bosch VIP X1**)

Значение в списке Протокол телеметрии	PTZ-протокол
Bosch	Bosch-Philips Receiver/Driver and Autodome Control Code Protocol
Panasonic-850	Panasonic WV-CS850/WV-CW860 Series
Pelco	Pelco Spectra D
Pelco P	Pelco Spectra P
Sensormatic	Sensormatic SpeedDome Ultra

П5.3 Подключение купольных камер к видеосерверам AXIS

При подключении купольной камеры к видеосерверам **AXIS** через последовательный порт (интерфейс RS232) укажите следующие параметры в настройках соответствующего объекта *PTZ-контроллер* (см. [Руководство администратора SecurOS](#)):

- **Протокол телеметрии** — выберите значение *Axis Native*;
- **Порт** — выберите порт на видеосервере, к которому подключена камера (COM1, COM2, ...);
- **Скорость, Четность, DTR, RTS** — значения полей не учитываются;
- **Использовать удаленное устройство** — активируйте поле и выберите из списка устройство видеозахвата, соответствующее видеосерверу **AXIS**.

Внимание! Идентификатор дочернего объекта *Поворотное устройство* должен быть равен идентификатору аналоговой камеры, указанному в собственных настройках видеосервера **AXIS** (см. рис. 63, поле **Device ID**), при подключении камеры к серверу через последовательный порт.

Приложение 5. Установка аппаратного обеспечения сторонних производителей

COM Port RS232

Port Settings

Usage: Pan Tilt Zoom

Port Options...

PTZ Driver Management

Current driver for this port: Pelco

Version: 2.03

Change or install new driver: Upload...

Video Source Configuration

Use with source:

☒ Video 1

☐ Video 2

☐ Video 3

☐ Video 4

Apply

Connected sources:

Video 1

Device ID: 1

Device Type: Generic

Specify advanced device settings [here](#).

Save Reset

Рис. 63. Определение порта, протокола и идентификатора камеры в настройках видеосервера **AXIS**

В собственных настройках видеосервера **AXIS** выполните следующие действия:

1. Перейдите на страницу настройки параметров последовательного порта (см. рис. 63; раздел **System Options**, подраздел **Ports & Devices**, далее выберите **RS232/PTZ**).
2. Выберите значение **Pan Tilt Zoom** в списке **Usage** раздела **Port Settings**.
3. Установите драйвер порта, соответствующий типу подключенной камеры (например, **Pelco**) в разделе **PTZ Driver Management** (нажмите кнопку **Upload** для загрузки драйверов с сайта компании **Axis**).
4. Активируйте поле, соответствующее тому видеоканалу, к которому подключена купольная камера, в разделе **Video Source Configuration** (в случае многоканальных видеосерверов).
5. Нажмите кнопку **Save** для сохранения настроек.

П5.4 Особенности подключения некоторых видеокамер и HUB-устройств

Выполните дополнительные действия для настройки подключения следующих видеокамер:

- IP-камеры **Smartec** и видеосерверы **ACTi** — для корректной работы необходимо установить видеокодек Xvid (см. www.xvid.org) на компьютер сети SecurOS, где созданы объекты *Устройство видеозахвата*, соответствующие данным устройствам.
- Все модели видеокамер **AXIS** — допускается создание только одного дочернего объекта *Камера* для объекта *Устройство видеозахвата*, соответствующего данному устройству (см. [Руководство администратора SecurOS](#)).
- Видеокамеры **Mobotix** с двумя объективами — для корректного приема видеосигнала от обоих объективов необходимо установить значение *Both* для параметра **Сигнал** в настройках соответствующего объекта *Устройство видеозахвата* (см. [Руководство администратора SecurOS](#)) и создать два дочерних объекта *Камера* с номерами каналов 1 и 2; при этом камера на канале 1 будет отображать видео с левого объектива, а камера на канале 2 — с правого объектива.

Приложение 6. Совместимость аппаратного обеспечения

П6.1 Системные платы

Таблица 29. Протестированные системные платы

Системная плата	Совместимость
A8-SQ800	Да
ABIT KG7-Lite SocketA	Да
ASUS 880KT	Да
ASUS A7N266-E	Да
ASUS A7N8X Deluxe	Да
ASUS A7V133	Да
ASUS A8V WI-FI Edition	Да
ASUS CUR-DLS Dual FC-PGA ATX RTL	Да
ASUS K8N-E	Да
ASUS K8S-MX	Да
ASUS K8V Deluxe	Да
ASUS P4C800	Да
ASUS P4G8X	Да
ASUS P4P800	Да
ASUS P4P800 SE	Ограниченная совместимость ¹
ASUS P4PE	Да
ASUS P5GPL	Ограниченная совместимость ²
Chaintech 7AJA	Да

(продолжение на следующей странице)

¹Невозможно установить более двух плат видеозахвата TVISS1-02.

²Невозможно установить более двух плат видеозахвата TVISS1-02.

Приложение 6. Совместимость аппаратного обеспечения

(начало на предыдущей странице)

Системная плата	Совместимость
EliteGroup ECS K7S6A	Да
EPOX EP-8KDA3J	Да
Gigabyte GA-K8NF-9	Да
Gigabyte GA-8I915P-D Pro	Да
Gigabyte GA-K8N Ultra-9	Да
Gigabyte GA-7VTXE	Да
Gigabyte GA-8IG	Да
Gigabyte GA-8IR2003	Да
Gigabyte GA-8S650GXM	Да
Intel Ashland 2 D845GVAD2	Да
Intel Billings 2 D845EBG2	Да
Intel Pendleton 2 D845EPT2	Да
Intel Rock Lake D865PERL	Да
Intel Silver Reef D845PESV	Да
Intel SE7320SP2	Нет
Intel SE7520BD2	Нет
Intel SE7525GP2	Да ³
Iwill XP4	Да
MSI 865PE Neo2-PS (MS-6728 v2.0)	Да
MSI Hetis 865GV 10/100-Lite (MSI MS-6765)	Да
Supermicro P3TDE6	Да
Supermicro P4DP6	Да
Supermicro SUPER P4SCT	Нет
Supermicro X5DA8	Да
TYAN S2460 Tiger MP	Да

(продолжение на следующей странице)

³Необходимо обновить BIOS (версия P9).

Приложение 6. Совместимость аппаратного обеспечения

(начало на предыдущей странице)

Системная плата	Совместимость
TYAN S2466 Tiger MPX	Да
VIA EPIA M	Да
TYAN Thunder i7525 (S2676)	Да ⁴

П6.2 Поворотные устройства

Таблица 30. Протестированные поворотные устройства

Поворотный контроллер	Совместимость
VideoTec DTMRX1	Да
VideoTec DCRX	Да
VideoTec DTRX	Да
VideoTec DCMRX	Да

Таблица 31. Интегрированные PTZ-протоколы

PTZ-протокол	Совместимость
American Dynamics 2150	Да
AXIS HTTP API v.2	Да
Bosch-Philips Receiver/Driver and Autodome Control Code Protocol	Да
CBC SMD	Да
C&B-A(V)N(P)800 Series	Да
Dongyang Unitech CCTV Receiver Control	Да
DynaColor Surveillance Control	Да

(продолжение на следующей странице)

⁴Требуется дополнительный драйвер для платы видеозахвата. Обратитесь в Службу технической поддержки (см. раздел [Обращение за технической поддержкой](#) на стр. 6).

Приложение 6. Совместимость аппаратного обеспечения

(начало на предыдущей странице)

PTZ-протокол	Совместимость
FastraX II PTZ	Да
Ganz ZC	Да
JVC TK-C676(A)/TK-C655(A)	Да
Kocom PTZ Control Protocol	Да
KPC301	Да
LG Remote Control Protocol	Да
LG SD 168HM PTZ Protocol	Да
Merit-Lilin FastDome Protocol	Да
Mobotix PTZ Protocol	Да
Panasonic WV-CSR600	Да
Panasonic WV-CS850/WV-CW860 Series	Да
Panasonic WV-CS950/CS960 Series	Да
Pelco CM6700	Да
Pelco D	Да
Pelco P	Да
PIV-6732	Да
QuarterBack Controller	Да
Samsung SCC-B2303	Да
Samsung SPD 1600	Да
Sensormatic	Да
SONY SNC-RZ25N/P CGI Command Protocol	Да
SONY SNC-Z20 CGI Command Protocol	Да
TED	Да
Universal AVIV	Да
Videotec DTRX, DCRX, DTMRX, DCMRX	Да

П6.3 Модемы с поддержкой голосовых сообщений

Таблица 32. Протестированные модемы

Модем с поддержкой голосовых сообщений	Совместимость
TRENDnet TFM-560U	Да
ZYXEL Omni 56k DUO	Да ⁵
Acorp Sprinter56k USB V.92 USB Modem	Да
USRobotics 56K Message	Да

⁵Некоторые из версий прошивки EEPROM для данного модема несовместимы с SecurOS. Драйвер совместим, если он регистрирует команды модема в системный регистр и устанавливает аудиодрайвер Unimodem.

Приложение 7. Системные утилиты

В комплект поставки SecurOS входит ряд дополнительных программ. Они находятся в корневом каталоге SecurOS или в подкаталоге \Tools папки SecurOS:

- утилита **ISS Hardware Report** (HardwareReportUtility.exe) составляет отчет обо всех установленных на данный компьютер платах видеозахвата TVISSxx и ключах Guardant (см. раздел [П7.1 Утилита ISS Hardware Report](#) на стр. 90);
- утилита **ISS System Report** (ISSInfo.exe) предназначена для сбора системной информации, необходимой для Службы технической поддержки (см. раздел [П7.2 Утилита ISS System Report](#) на стр. 91);
- утилита **ISS Media Export** (Backup.exe) воспроизводит архивное видео/аудио, экспортирует выделенную часть архива в файлы формата AVI, ASF и BMP (см. [Руководство администратора SecurOS](#));
- утилита **gtUSB Configuration** (gtusbconfig.exe) предназначена для настройки USB-устройств видеозахвата (см. [Руководство администратора SecurOS](#));
- утилита **ISS Startup Configuration** (RegService.exe) прописывает SecurOS как сервис Windows или как обычное приложение (см. раздел [П7.3 Утилита ISS Startup Configuration](#) на стр. 93);
- утилита **DSAdmin** (dsadmin.exe) предназначена для определения используемых баз данных (см. раздел [П7.4 Утилита DSAdmin](#) на стр. 94);
- утилита **ISS Database Update** (idb.exe) предназначена для доступа к базе данных (см. [Руководство администратора SecurOS](#));
- утилита **ISS Object Types Database Editor** (DDI.exe) редактирует базу данных типов объектов SecurOS (это не действующая база данных) (см. [Руководство администратора SecurOS](#)).

П7.1 Утилита ISS Hardware Report

Нахождение на диске:

<корневой каталог SecurOS>\Tools\HardwareReportUtility.exe

Запуск через главное меню:

Пуск → Программы → SecurOS → Информация об устройствах

Эта утилита определяет все установленные на данный компьютер платы видеозахвата TVISSxx и ключи Guardant (см. рис. 64). Составляемый с помощью утилиты отчет необходим для генерации файла лицензионного ключа (key.iss) Службой технической поддержки компании ISS.

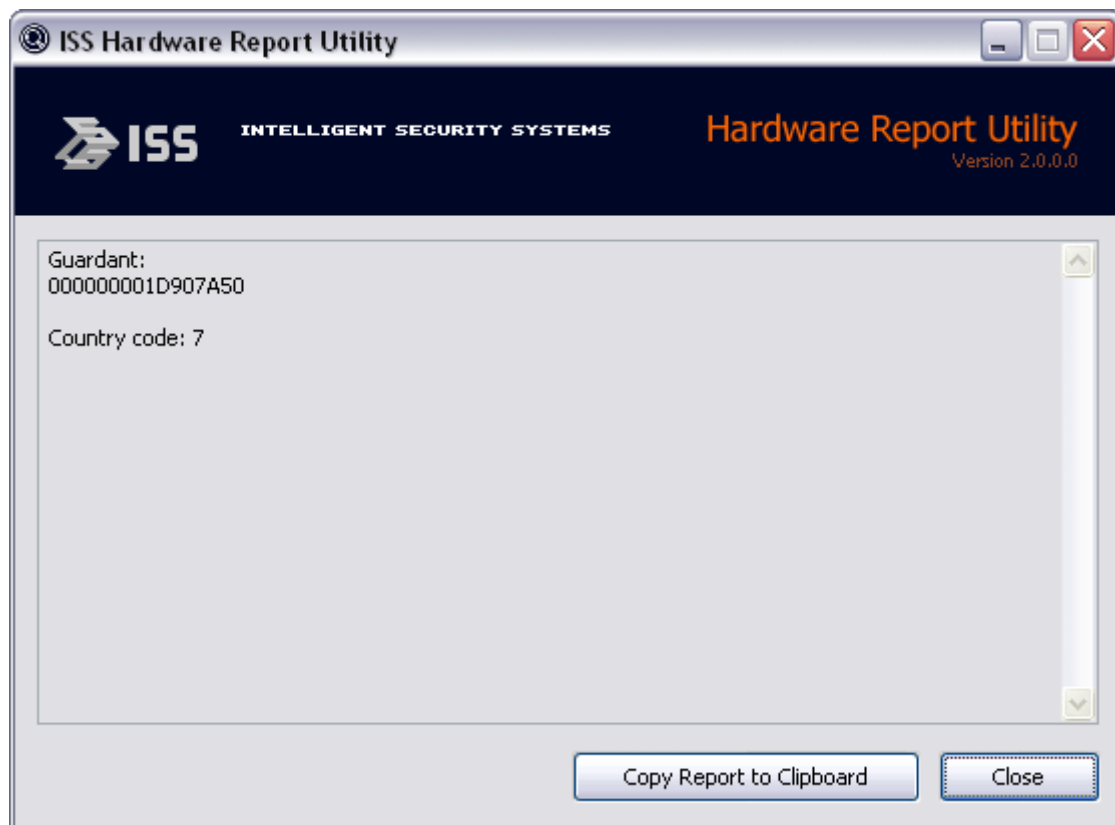


Рис. 64. Результат запроса утилиты ISS Hardware Report

Чтобы записать отчет утилиты в файл:

1. Нажмите кнопку **Copy Report to Clipboard** в окне утилиты.
2. Создайте пустой текстовый файл в любой программе редактирования текстовых файлов (Блокнот, Microsoft Word и т. д.).
3. Вставьте содержимое буфера обмена и сохраните файл отчета.

Утилита также может быть использована для диагностики дополнительного аппаратного обеспечения и сопутствующих драйверов: если идентификатора устройства нет, то это означает некорректность установки драйверов.

П7.2 Утилита ISS System Report

Нахождение на диске:

<корневой каталог SecurOS>\Tools\ISSInfo.exe

Данная утилита предназначена для сбора информации о системе SecurOS и компьютере (см. рис. 65). Такая информация может понадобиться, например, специалистам технической поддержки при устранении каких-либо неполадок в системе.

Утилита **ISS System Report** собирает следующую информацию:

Приложение 7. Системные утилиты

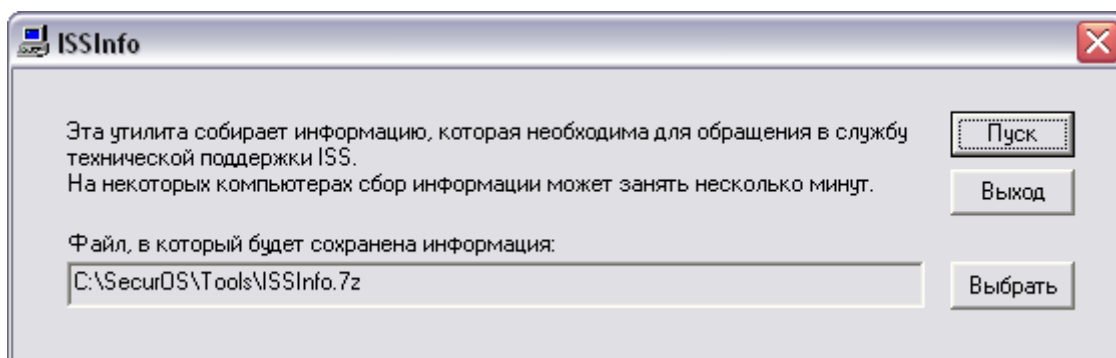


Рис. 65. Окно утилиты ISS System Report

- в файле `current_modules` содержится перечень dll- и exe-файлов с указанием их версии из папки SecurOS;
- в файле `current_driver` записана информация о версии установленного драйвера плат TVISSx;
- в файле `DallasCodes` записана информация о кодах установленных устройств (TVISSx или Guardant);
- в файле `ISS_Config` содержится информация раздела реестра `HKEY_LOCAL_MACHINE\SOFTWARE\ISS`;
- в файлах `data`, `videoi`, `protocol` содержится информация из БД `securos`, `fsindex` и `protocol` соответственно;
- в файле `SystemInfo` записана информация о компьютере, на котором установлен SecurOS и на котором данная утилита была запущена.

Во вложенной папке `\ISSInfo\cur` хранятся лог-файлы модулей, дамп-файлы, файлы программ и скриптов, а также ключевой файл `key.iss`.

Во вложенной папке `\ISSInfo\PerfomanceMonitor` хранится информация, собранная объектом *System Statistics*, если он когда-либо был настроен.

Во вложенной папке `\ISSInfo\system32` лежат файлы системных библиотек.

Примечание. Утилита **ISS System Report** собирает только вышеперечисленную информацию.

Чтобы начать сбор системной информации, нажмите кнопку **Пуск**.

Вся собранная информация будет сохранена в созданный подкаталог `\Tools\ISSInfo`. Его содержимое будет упаковано в архив. Используя кнопку **Выбрать**, можно указать файл и место, в которое следует производить архивацию.

П7.3 Утилита ISS Startup Configuration

Нахождение на диске:

<корневой каталог SecurOS>\Tools\RegService.exe

Утилита предназначена для назначения SecurOS как сервиса Windows или как обычного приложения Win32 (см. рис. 66). Если выбрано значение `Run as service`, то SecurOS будет запускаться автоматически при каждом запуске Windows.



Рис. 66. Окно утилиты ISS Startup Configuration

Для точной настройки SecurOS как сервиса Windows рекомендуется использовать утилиту **SecurOS Control Service**, непосредственно запускающую SecurOS в режиме сервиса.

Нахождение на диске:

<корневой каталог SecurOS>\securos_svc.exe

При запуске этой утилиты из командной строки с параметром `-h` появится справочная информация по синтаксису и переменным.

Синтаксис утилиты **SecurOS Control Service**:

`securos_svc -h -i n -r -s -k -t n -u s -p s -l s -d`

- `-h` — выдается список ключей утилиты;
- `-i n` — зарегистрировать SecurOS как сервис Windows. Укажите тип запуска службы `n` (1 — выключен, 2 — автоматический, 3 — ручной запуск);
- `-r` — удалить службу из списка служб Windows;
- `-s` — запустить службу;
- `-k` — остановить службу;
- `-t` — укажите тип запуска зарегистрированной службы (1 — выключен, 2 — автоматический, 3 — ручной запуск);
- `-u s` — задать имя пользователя `s` для запуска службы;
- `-p s` — задать пароль пользователя `s` для запуска службы;

Приложение 7. Системные утилиты

- `-l s` — задать имена зависимых служб;
- `-d` — включить информационный режим (режим отладки).

Для корректного старта сервиса SecurOS рекомендуется зарегистрировать SecurOS как автоматически запускаемую службу и установить зависимость службы СУБД PostgreSQL:

```
securos_svc.exe -i 2 -l "pgsql-8.3"
```

Необходимо проверить истинное имя службы PostgreSQL на данном компьютере (в примере использовано имя `pgsql-8.3`).

Чтобы найти имя службы PostgreSQL:

1. Откройте **Панель управления** Windows (**Пуск** → **Настройка** → **Панель управления**).
2. Выберите **Администрирование**, далее **Службы**.
3. В списке служб найдите сервис **PostgreSQL8** и выберите **Свойства**. Имя службы указывается в поле **Имя службы**.

После регистрации сервис SecurOS при старте будет ожидать завершения запуска сервиса PostgreSQL.

Примечание. Рекомендуется использовать автоматический вход в Windows XP в случае настройки SecurOS как службы Windows (см. описание настройки автоматического входа в [Руководстве администратора SecurOS](#)).

П7.4 Утилита DSAdmin

Нахождение на диске:

```
<корневой каталог SecurOS>\dsadmin.exe
```

Утилита предназначена для хранения настроек объектов системы (база данных *Securos*), записи событий, происходящих в системе (база данных *Protocol*), и записи информации о тревогах и об установленных в видеоархиве закладках (база данных *fsindex*).

Примечание. Указанные выше базы данных определяются и прописываются в процессе установки SecurOS.

В окне утилиты присутствуют четыре поля для определения строк подключения к базам данных:

- **Basic Data** — строка подключения к общей базе данных для хранения настроек объектов системы (база данных *Securos*);
- **Protocol** — строка подключения к базе данных событий, происходящих в системе (база данных *Protocol*);

Приложение 7. Системные утилиты

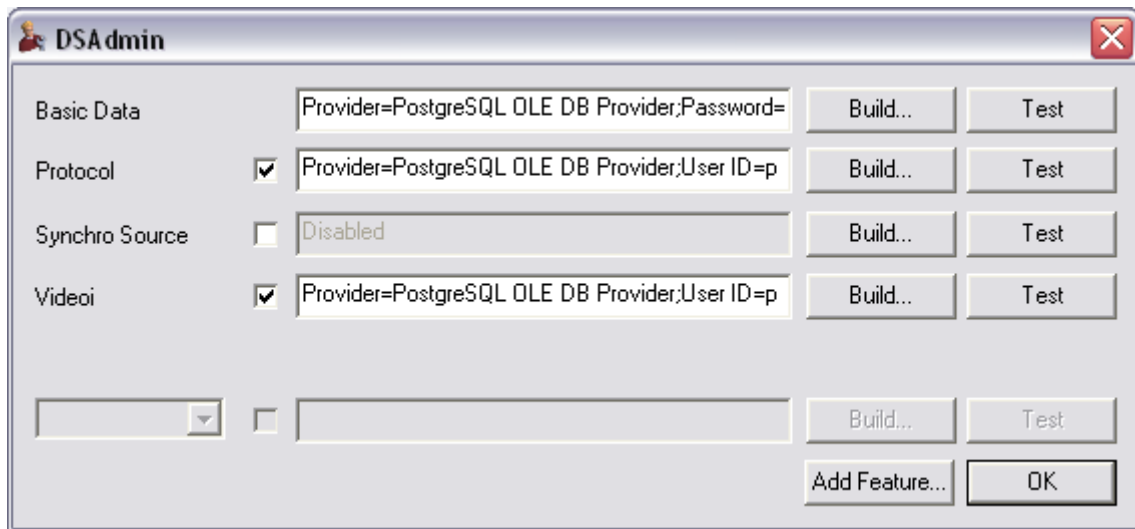


Рис. 67. Окно утилиты DSAdmin

- **Synchro Source** — строка подключения к синхронизируемой базе данных (опционально);
- **Videoi** — строка подключения к базе данных для хранения информации о тревогах и об установленных в видеоархиве закладках (база данных fsindex).

Примечание. При необходимости можно задать и настроить дополнительную базу данных в поле **New feature**.

*Чтобы изменить строку подключения, нажмите соответствующую кнопку **Build**. Чтобы проверить соединение с базой данных, — нажмите кнопку **Test**.*

При нажатии кнопки **Build** откроется окно **Свойства связи с данными** для автоматической настройки строки соединения с базой данных в соответствии с указанными в закладках параметрами:

- закладка **Поставщик данных**: выберите **PostgreSQL OLE DB Provider** из списка;
- закладка **Подключение**:
 - пропишите название сервера или адрес в поле **Источник данных** (например, 127.0.0.1, localhost);
 - пропишите название базы данных в поле **Размещение** (например, securos_db);
 - пропишите данные учетной записи, ранее созданной в СУБД, в полях **Пользователь** и **Пароль** соответственно.

*Чтобы сохранить изменения, нажмите кнопку **ОК**. Изменения будут применены и окно утилиты закроется.*

Глоссарий

CCTV (Closed Circuit Television) — телевизионная система, предназначенная для ограниченного количества пользователей (кабельное телевидение).

COM-порт — другое название последовательного порта компьютера, обычно использует интерфейс RS232.

DNS (Domain Name System) — доменная система именования.

Guardant — лицензионный ключ (на USB-порт). Необходим для рабочего места администратора сети безопасности SecurOS.

PCI — тип используемого в компьютере слота расширения.

SecurOS (Security Operating System) — операционная система безопасности, предназначенная для создания глобальной физической системы безопасности, которая включает в себя (но не ограничивается этим) видеонаблюдение, аудиомониторинг (контроль звукового сопровождения), контроль доступа.

WINS (Windows Internet Name System) — Windows-служба интернет-имен.

Биометрическая идентификация — идентификации пользователя, основанная на уникальности характеристик человеческого тела, например отпечатки пальцев.

Ведущий сервер — сервер приложения, с которого копируется база данных конфигурации. Используется для первоначального подключения других серверов приложения и рабочих мест администратора к сети безопасности SecurOS.

Видеоплата (плата видеозахвата) — часть аппаратного обеспечения для преобразования видеосигналов в цифровой формат, плата оцифровки видеоизображений.

Видеосервер — сервер приложений, оборудованный одной или несколькими платами видеозахвата с подключенными видеокамерами.

Выделение (распознавание) лица — технология, позволяющая выделить лицо человека из потока живого видео или статического изображения для его сравнения и соответствия с существующей базой фотоданных и, таким образом, определить сходство. Распознавание лица является частью биометрической идентификации.

Интегрированная система безопасности — программное обеспечение, объединяющая и устройства разных производителей, и модули распознавания в единую систему.

Модуль — часть представленной системы безопасности, выполняющая определенные функции внутри нее.

Охранно-пожарная система — пассивная система управления, предупреждающая о незаконных и опасных действиях (пожар, разбитое окно и т. д.).

Поворотное устройство — устройство, способное динамически изменять свою ориентацию в пространстве и управляемое командами оператора (человека) или автоматизированной системой управления.

Протокол TCP/IP — сетевой протокол.

Рабочее место администратора (или оператора) — клиентский компьютер, подсоединенный к сети безопасности SecurOS, с которого можно проводить конфигурирование (или только мониторинг) системы.

Распознавание номера автомобиля — технология, позволяющая распознавать номера автомобилей, в режиме живого видео или статического изображения.

Сервер приложений — компьютер, ответственный за поддержку и управление определенной части сети безопасности.

Сеть безопасности SecurOS (сеть безопасности) — серверы SecurOS и рабочие места, соединенные в единую сеть по протоколу TCP/IP.

Система контроля доступа — комплекс аппаратного и программного обеспечения для охраны территорий и зданий от несанкционированного доступа.

Системный интегратор — человек или организация, ответственная за установку (поддержку) системы безопасности.

Служба технической поддержки — группа людей, помогающих пользователям устанавливать, поддерживать и работать с сетью безопасности SecurOS.

Файл лицензионного ключа — файл, содержащий информацию о конфигурации авторизованной системы.

Предметный указатель

A

Adobe Reader, [6](#)

D

DSAdmin Utility, утилита, [50](#)

DSAdmin, утилита, [90](#)

G

gtUSB Configuration, утилита, [90](#)

I

IP-камера, [10](#), [20](#), [22](#)

ISS Database Update, утилита, [90](#)

ISS Hardware Report, утилита, [90](#)

ISS Media Export, утилита, [90](#)

ISS Object Types Database Editor, утилита, [90](#)

ISS Startup Configuration, утилита, [90](#)

ISS System Report, утилита, [50](#), [90–92](#)

P

PgAdmin III, утилита, [36](#), [50](#)

PostgreSQL, [31](#)

PTZ-контроллер, объект, [81](#), [82](#)

S

SecurOS Control Service, утилита, [93](#)

System Statistics, объект, [92](#)

В

видео-HUB, [22](#)

видеоконцентратор, [12](#), [14](#)

видеоплата, [19](#), [20](#)

видеосервер, [20](#)

выгрузка, [48](#)

К

Камера, объект, [42](#), [84](#)

Компьютер, объект, [47](#)

к

ключ Guardant, [90](#)

л

лицензионный ключ, [90](#)

ключ Guardant, [12](#), [19](#)

файл key.iss, [12](#), [26](#)

М

Монитор, объект, [47](#)

О

Объект охраны, объект, [47](#)

П

Поворотное устройство, объект, [81](#), [82](#)

п

поворотное устройство, [10](#)

купольная камера, [22](#)

протокол RDP, [10](#)

р

рабочее место, [9](#), [10](#), [12](#), [14](#)

рабочее место администратора, [10](#)

рабочее место оператора, [10](#)

с

сервер, [9](#), [12](#), [18](#), [19](#)

ведущий, [45](#), [51](#)

видеосервер, [10](#)

сервер приложений, [10](#)

сетевое окружение, [9](#)

системная плата, [17](#), [19](#), [21](#)

системные требования, [16](#)

т

техническая поддержка, [6](#), [26](#), [90](#)

у

Устройство видеозахвата, объект, [81](#), [84](#)

у

удаленное соединение Microsoft, [10](#)

установка

 видеокамеры, [21](#)

 видеоплата, [20](#)

 звуковая плата, [24](#)

 лицензионный ключ key.iss, [34](#)

 микрофоны, [24](#)

 охранно-пожарная подсистема, [24](#)

 поворотное устройство, [22](#)

 подсистема контроля доступа, [24](#)

 подсистема оповещения, [24](#)

 программное обеспечение, [25](#)

 язык интерфейса, [34](#)

учетная запись

 postgres, [36](#)

э

Экран, объект, [47](#)

