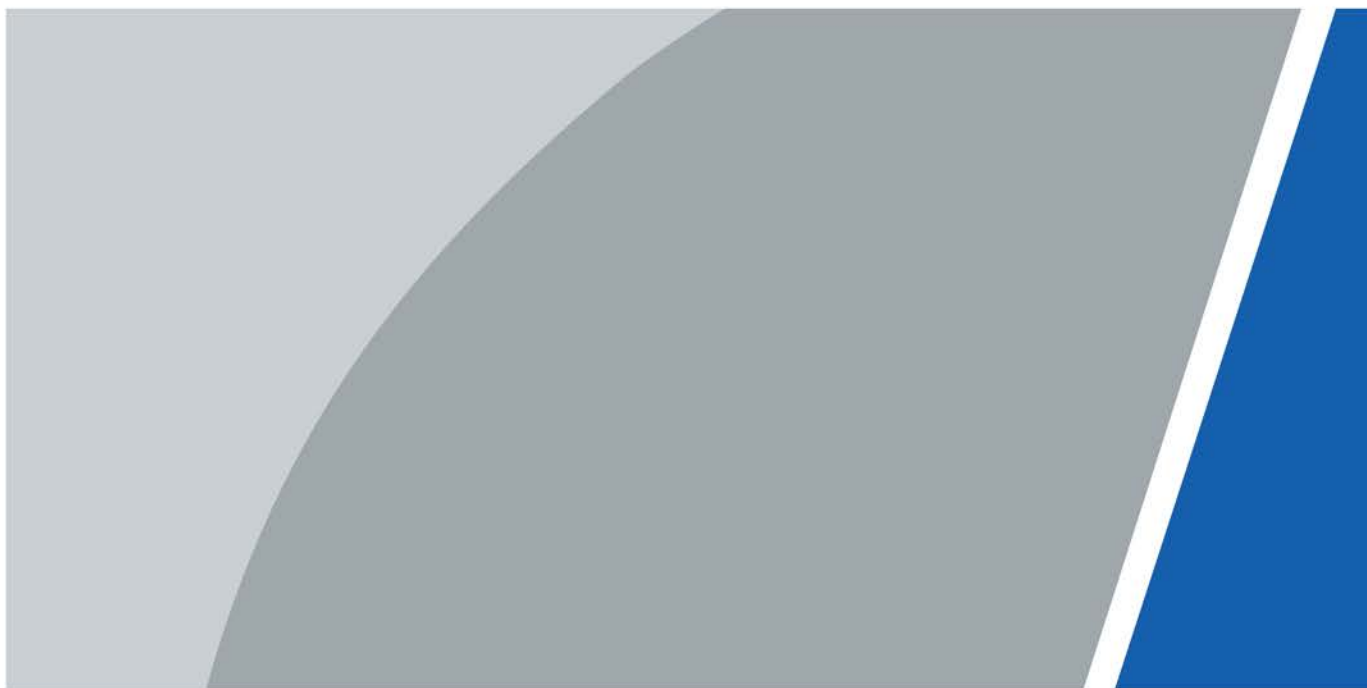


# **Сетевой видеорегистратор**

## **Краткое руководство пользователя**



V1.0.0





# Предисловие

## Общие сведения

В настоящем кратком руководстве (далее именуемом «Руководство») приведены сведения о функциях и операциях цифрового видеорегистратора (далее именуемого NVR).

## Указания по технике безопасности

В руководстве могут появляться следующие разбитые на категории сигнальные слова с определенным значением.

Сигнальные слова	Значение
 <b>ОПАСНОСТЬ!</b>	Указывает на потенциально опасную ситуацию с высокой степенью риска, которая, если ее не предотвратить, приведет к смерти или серьезной травме.
 <b>ПРЕДУПРЕЖДЕНИЕ!</b>	Указывает на потенциально опасную ситуацию со средней и низкой степенью риска, которая, если ее не предотвратить, может привести к травме легкой или средней степени тяжести.
 <b>ВНИМАНИЕ!</b>	Указывает на потенциально опасную ситуацию, которая, если ее не предотвратить, может привести к повреждению собственности, потере данных, снижению производительности или непредвиденным результатам.
 <b>СОВЕТЫ</b>	Предоставляет способы решения проблемы или позволяет сэкономить ваше время.
 <b>ПРИМЕЧАНИЕ</b>	Предоставляет дополнительную информацию для выделения и дополнения основного текста.

## История изменений

Версия	Содержание изменения	Дата выпуска
V1.0.0	Первый выпуск.	Июль 2020 года

## Уведомление о защите конфиденциальности

Являясь пользователем NVR или контроллером данных, вы можете собирать личные данные других людей, такие как изображения лиц, отпечатки пальцев, номерные знаки автомобилей, адреса электронной почты, номера телефонов и сведения GPS о местоположении. Вы должны соблюдать местные законы и постановления об обеспечении конфиденциальности для защиты законных прав и интересов других людей путем принятия адекватных мер, включая, помимо прочего, предоставление четкой и ясной информации субъекту данных о существующей области контроля и предоставление соответствующих контактных данных.

## О данном руководстве

- Настоящее руководство предназначено только для справки. В случае несоответствия между Руководством и фактическим продуктом преимущественную силу имеют характеристики и параметры фактического продукта.
- Мы не несем ответственности за убытки, вызванные операциями, выполненными с нарушением требований настоящего Руководства.
- Руководство будет обновляться в соответствии с последними законами и постановлениями, действующими в соответствующих регионах. Для получения подробной информации см. печатное руководство, руководство на CD-ROM, отсканируйте QR-код или посетите наш официальный сайт. В случае несоответствия между бумажной копией и электронной версией руководства преимущественную силу имеет электронная версия.
- Все варианты конструкции и программное обеспечение могут быть изменены без предварительного письменного уведомления. Обновления продукта могут привести к некоторым различиям между функциями фактического продукта и функциями, описанными в Руководстве. Свяжитесь со службой поддержки клиентов для получения последней версии программы и дополнительной документации.
- При этом не исключаются отклонения в технических характеристиках, функциях и описании операций, а также ошибки при печати. Если возникнут какие-либо сомнения или споры, руководствуйтесь нашим окончательным объяснением.
- Если не удастся открыть Руководство (в формате PDF), обновите существующее программное обеспечение для чтения документов или попробуйте использовать другое аналогичное ПО.
- Все товарные знаки, зарегистрированные товарные знаки и названия компаний, упомянутые в Руководстве, являются собственностью соответствующих владельцев.
- Если при использовании NVR возникла проблема, посетите наш веб-сайт, обратитесь к продавцу или в службу поддержки клиентов.
- При возникновении сомнений или спорных ситуаций обратитесь к производителю.

# Важные меры предосторожности и предупреждения

В следующем разделе приведено описание надлежащего применения сетевого видеорежистратора. Внимательно прочтите настоящее Руководство перед использованием устройства, чтобы предотвратить травмы и материальный ущерб. Строго соблюдайте требования руководства во время эксплуатации устройства и сохраните его после прочтения.

## Эксплуатационные требования

- Камеры PoE предназначены для установки в помещениях.
- Не устанавливайте NVR в местах, подверженных воздействию прямых солнечных лучей, или рядом с тепловыделяющими устройствами.
- Не устанавливайте сетевой видеорежистратор во влажных, пыльных или грязных местах.
- Обеспечьте горизонтальную установку или устанавливайте устройство в устойчивых местах, не допуская его падения.
- Не допускайте попадания брызг жидкости на NVR. Не кладите на него емкости, наполненные жидкостью, чтобы эта жидкость не проникла внутрь устройства.
- Устанавливайте NVR в хорошо вентилируемых местах и не закрывайте его вентиляционное отверстие.
- Используйте NVR только в пределах номинального диапазона входных и выходных напряжений.
- Не разбирайте NVR самостоятельно.
- Транспортируйте, используйте и храните NVR с соблюдением допустимого диапазона влажности и температуры.

## Питание

- Используйте батареи в соответствии с установленными требованиями. В противном случае возможно возгорание или взрыв батарей!
- Для замены батарей используйте только батареи того же типа.
- Утилизируйте отслужившие батареи в соответствии с инструкциями.
- Используйте электрические провода с номинальными характеристиками, рекомендованными местными правилами.
- Используйте стандартный адаптер питания, соответствующий конкретной модели NVR. В противном случае возможны травмы или повреждения NVR.
- Используйте источник питания, отвечающий требованиям SELV (безопасное сверхнизкое напряжение), и подавайте питание с номинальным напряжением, которое соответствует требованиям стандарта IEC60950-1 к источникам ограниченной мощности. Конкретные требования к источнику питания см. на этикетках устройства.
- Изделия категории I подключаются к сетевой розетке, имеющей защитное заземление.
- Устройство сопряжения является отключающее устройство. Во время обычного использования установите угол наклона, облегчающий работу.

# Содержание

Предисловие .....	I
Важные меры предосторожности и предупреждения.....	III
1 Локальная работа.....	1
1.1 Запуск NVR.....	1
1.2 Инициализация NVR.....	1
1.3 Настройка сетевых параметров .....	5
1.4 Добавление IP-камеры .....	6
1.4.1 Инициализация IP-камеры .....	6
1.4.2 Добавление IP-камеры по результату поиска .....	10
1.4.3 Добавление IP-камеры вручную.....	12
1.5 Настройка расписания хранения записанного видео.....	15
1.6 Настройка параметров P2P .....	18
1.6.1 Включение функции P2P.....	18
1.6.2 Добавление сетевого видеорегистратора в клиентскую программу смартфона.....	19
1.7 Интеллектуальное обнаружение движения.....	21
1.8 Просмотр в реальном времени .....	24
1.9 Запись в процессе воспроизведения .....	25
2 Вход в Интернет .....	错误!未定义书签。
Приложение 1 Рекомендации по кибербезопасности .....	28

# 1 Локальная работа



В интерфейсах разных моделей могут быть небольшие различия. Следующие рисунки приведены только для справки. Все зависит от конкретного изделия.

## 1.1 Запуск NVR

Перед запуском NVR убедитесь в нижеследующем.

- Номинальное входное напряжение соответствует требованиям к электропитанию сетевого видеорежистратора.
- Провода для подключения питания готовы.
- Для защиты устройства сначала подключите NVR к адаптеру питания, а затем подключите адаптер к розетке.
- Всегда используйте источник со стабильным током. В качестве источника питания рекомендуется использовать ИБП.

## 1.2 Инициализация NVR

В этом разделе описана процедура инициализации NVR перед использованием.

### Исходная информация

При первой загрузке вам необходимо установить пароль для пользователя **admin** (администратор, используется по умолчанию). Чтобы гарантировать безопасность устройства, мы настоятельно рекомендуем хранить пароль для входа в систему надлежащим образом и регулярно изменять его.

### Процедура

Шаг 1: Включите сетевой видеорежистратор.

Откроется интерфейс инициализации устройства.

Шаг 2: В раскрывающихся списках выберите нужный регион, язык и стандарт видео.



Вы можете изменить эти параметры на страницах настроек NVR после инициализации.

Рис. 1–1 Настройка местоположения, языка и стандарта видео

The screenshot shows a 'Device Initialization' window with a dark background. A light gray box labeled '1' contains three settings: 'Region' with a dropdown menu showing 'Please select an item.', 'Language' with a dropdown menu showing 'English', and 'Video Standard' with a dropdown menu showing 'PAL'. At the bottom right, there is a button labeled 'Next' with a small orange circle labeled '2' next to it.

Шаг 3: Нажмите **Далее** (Next).

Шаг 4: Прочтите лицензионное соглашение по программному обеспечению и выберите пункт **Я принимаю все условия** (I have read and agree to all terms), а затем нажмите **Далее** (Next).

Шаг 5: Выберите часовой пояс и настройте системное время, а затем нажмите **Далее** (Next).

Рис.1–2 Настройка часового пояса и системного времени

The screenshot shows a 'Device Initialization' window with a dark background. A light gray box labeled '1' contains two settings: 'Time Zone' with a dropdown menu showing '(UTC+04:00) Yerevan' and 'System Time' with two input fields showing '2020 -01 -08' and '13 : 11 : 35'. At the bottom right, there is a button labeled 'Next' with a small orange circle labeled '2' next to it.

Шаг 6: Установите пароль для администратора устройства и нажмите **Далее** (Next).

Рис. 1–3 Установка пароля

Device Initialization

1. Password Setting → 2. Unlock Pattern → 3. Password Protection

1

Username admin

Password




Confirm Password

Password Hint

Password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters (Characters like ' " ; : & cannot be included in ).

2 Next

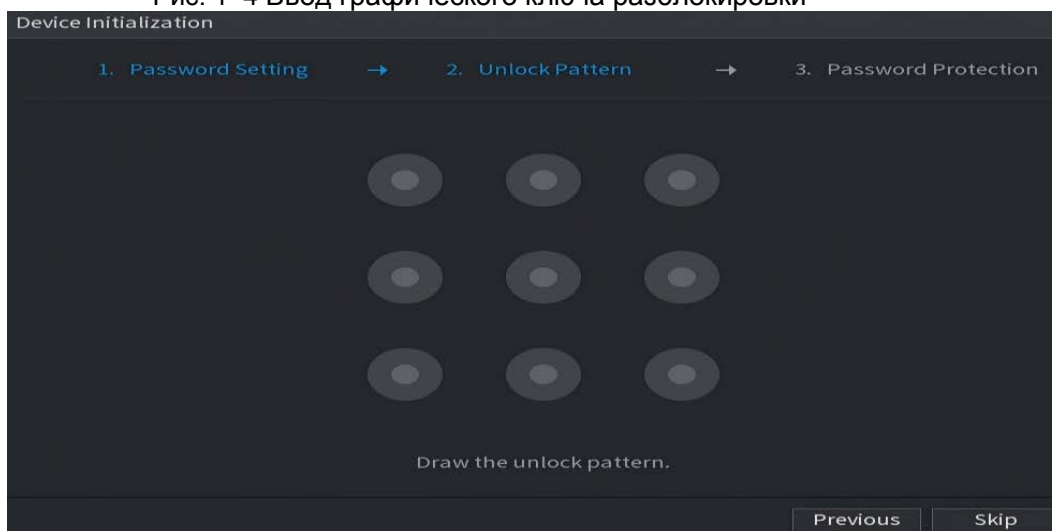
Таблица 1–1 Информация о пароле

Параметр	Описание
Имя пользователя	Пользователь по умолчанию: <b>admin</b> (администратор). Вы не можете его изменить.
Пароль	Введите новый пароль для администратора устройства в поле <b>Пароль</b> (Password) и подтвердите его в следующем поле.
Подтверждение пароля	 <p>Новый пароль может содержать от 8 до 32 символов как минимум двух из следующих категорий: буквы, цифры и специальные знаки (кроме «'», «"», «;», «:» и «&amp;»).</p>
Подсказка для пароля	<p>Введите контрольный вопрос, который поможет вам вспомнить пароль для вашего устройства.</p>  <p>В интерфейсе входа в систему нажмите . После этого появится подсказка, которая поможет сбросить пароль.</p>

Шаг 7: (Необязательно). Используйте мышь, чтобы нарисовать графический ключ разблокировки, а затем нарисуйте его еще раз для подтверждения.



Рис. 1–4 Ввод графического ключа разблокировки

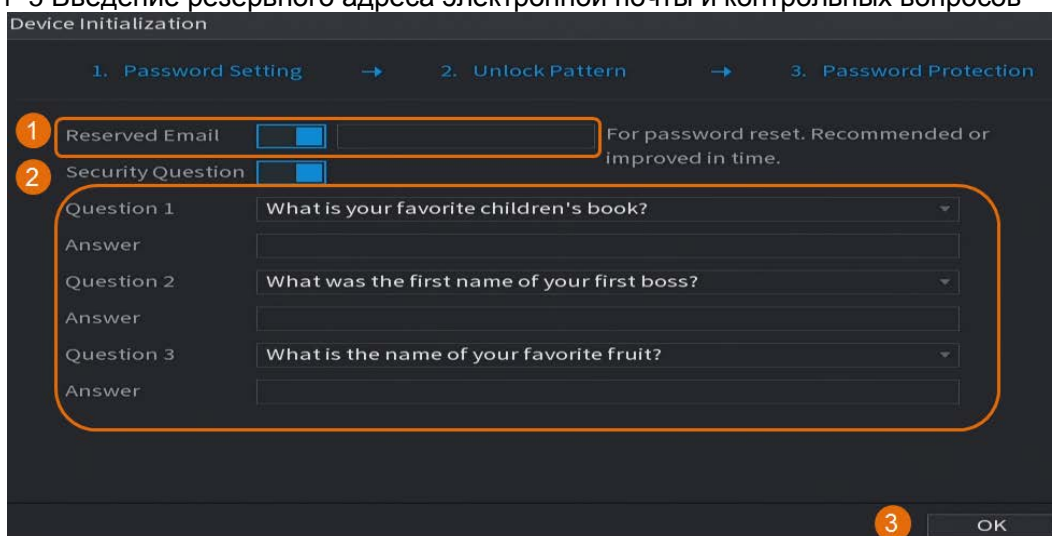


- Графический ключ должен пересекать не менее четырех точек.
- Если вы не хотите настраивать графический ключ для разблокировки, нажмите **Пропустить** (Skip).
- После установки графического ключа, он будет использоваться в качестве метода аутентификации по умолчанию. Если вы пропустите эту настройку, вам потребуется ввести пароль для входа.

Шаг 8: (Необязательно). Задайте резервный адрес электронной почты и контрольные вопросы для доступа к NVR.

- Активируйте опцию **Резервный адрес электронной почты** (Reserved Email) и введите адрес электронной почты.
- Активируйте опцию **Контрольный вопрос** (Security Question) и выберите вопросы из раскрывающихся списков **Вопрос 1**, **Вопрос 2** и **Вопрос 3** (Question 1, Question 2 и Question 3), а затем введите ответы на эти вопросы.

Рис. 1–5 Введение резервного адреса электронной почты и контрольных вопросов



Шаг 9: Нажмите **OK**.

# 1.3 Настройка сетевых параметров

Вы можете настроить основные параметры сети, такие как сетевой режим, версию IP и IP-адрес сетевого видеорегистратора.

Шаг 1: Выберите **Главное меню > СЕТЬ > TCP/IP** (Main Menu > NETWORK > TCP/IP).

Шаг 2: Настройте параметры.



Вы также можете настроить параметры сети в мастере запуска.

Рис. 1–6 TCP/IP

Таблица 1–2 Параметры TCP/IP

Параметр	Описание
Версия IP	В списке <b>Версия IP</b> (IP Version) можно выбрать <b>IPv4</b> или <b>IPv6</b> . Обе версии поддерживаются для доступа.
MAC-адрес	В этом поле отображается MAC-адрес сетевого видеорегистратора.
DHCP	Включение режима DHCP. После включения режима DHCP такие параметры как IP-адрес, маска подсети и шлюз по умолчанию будут недоступны для настройки. <ul style="list-style-type: none"><li>Если режим DHCP активен, полученная информация будет отображаться в полях <b>IP-адрес</b>, <b>Маска подсети</b> и <b>Шлюз по умолчанию</b>. (IP Address, Subnet Mask и Default Gateway). Если нет, во всех полях будет отображаться значение 0.0.0.0.</li><li>Если соединение PPPoE установлено успешно, IP-адрес, маска подсети, шлюз по умолчанию и DHCP будут недоступны для настройки.</li></ul>
IP-адрес	Введите IP-адрес, укажите соответствующую маску подсети и шлюз по умолчанию.  IP-адрес и шлюз по умолчанию должны находиться в одном сегменте сети.
Маска подсети	
Шлюз по умолчанию	

Параметр	Описание
Предпочтительный DNS	Введите IP-адрес DNS.
Альтернативный DNS	Введите IP-адрес альтернативного DNS.
MTU	<p>Введите значение MTU для сетевой карты. Это значение варьируется от 1280 до 1500 байт. Значение по умолчанию: 1500.</p> <p>Предлагаемые значения MTU приведены ниже.</p> <ul style="list-style-type: none"> <li>• 1500: самое большое значение для информационного пакета Ethernet. Это значение обычно выбирается, если нет соединений PPPoE или VPN. Это значение также устанавливается по умолчанию для некоторых маршрутизаторов, сетевых адаптеров и коммутаторов.</li> <li>• 1492: оптимизированное значение для PPPoE.</li> <li>• 1468: оптимизированное значение для DHCP.</li> <li>• 1450: оптимизированное значение для VPN.</li> </ul>
Проверка	Нажмите <b>Тест</b> (Test), чтобы проверить, совместим ли введенный IP-адрес со шлюзом.

Шаг 3: Нажмите **ОК**.

## 1.4 Добавление IP-камеры

Вы можете добавить IP-камеру, используя результаты поиска или введя IP-информацию вручную.



Камеры, которые вы хотите добавить, должны быть в одной сети с NVR.

### 1.4.1 Инициализация IP-камеры

В этом разделе описано, как инициализировать новые камеры или камеры, у которых были восстановлены заводские настройки по умолчанию.

#### Исходная информация

Перед подключением к сетевому видеорегистратору IP-камера должна быть инициализирована, в противном случае соединение не будет установлено. При инициализации изменяется пароль для входа в IP-камеру и IP-адрес.



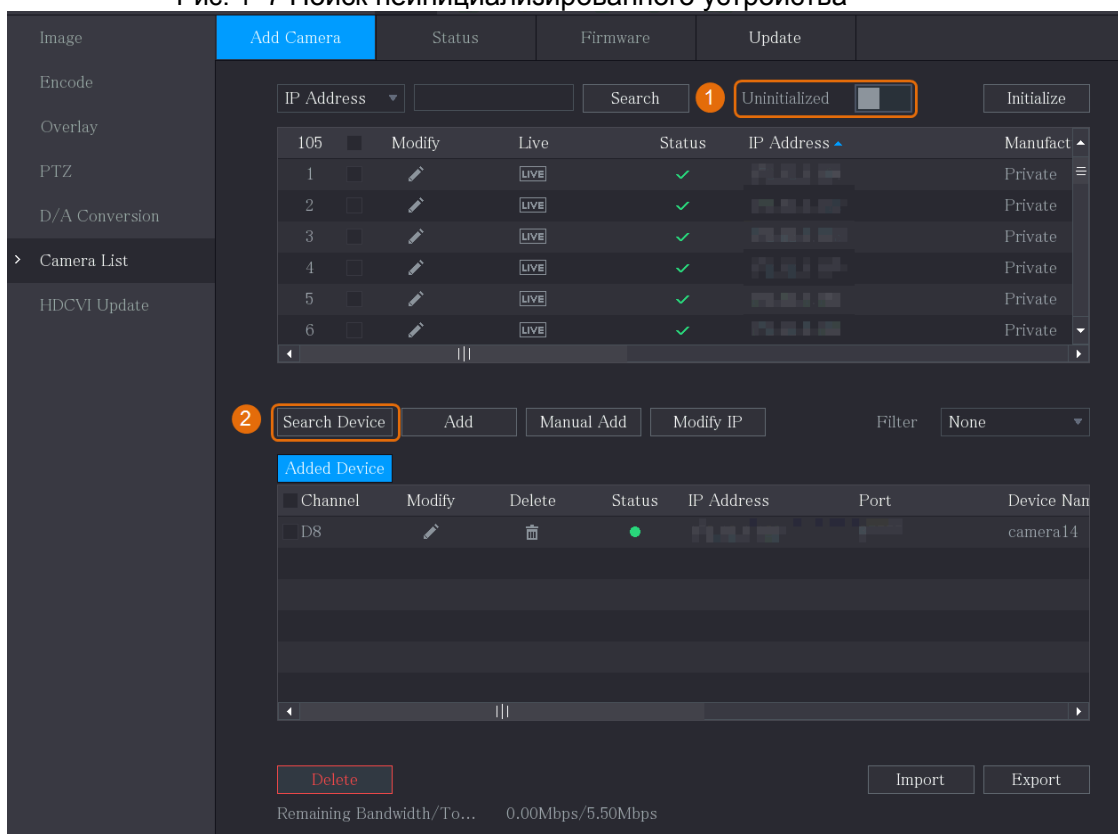
При подключении камеры к NVR через порт PoE видеорегистратор автоматически инициализирует камеру. Камера по умолчанию получает пароль и адрес электронной почты NVR.

#### Процедура

Шаг 1: Выберите **Главное меню > Камера > Список камер > Добавить камеру** (Main Menu > Camera > Camera List > Add Camera).

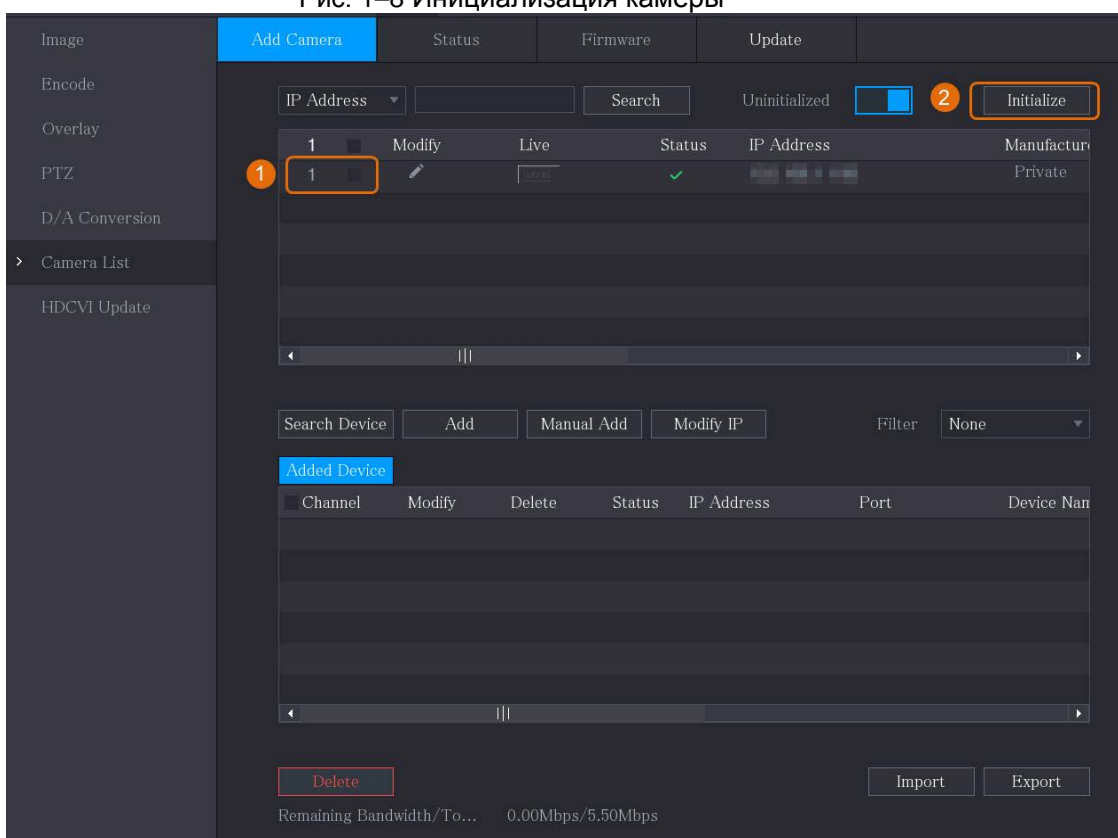
Шаг 2: Выберите **Не инициализировано** (Uninitialized), а затем нажмите **Поиск устройства** (Search Device).

Рис. 1–7 Поиск неинициализированного устройства



**Шаг 3:** Выберите камеру для инициализации и нажмите **Инициализировать** (Initialize).

Рис. 1–8 Инициализация камеры



**Шаг 4:** Установите пароль и адрес электронной почты для IP-камеры.

- Использование настроек сетевого видеорегистратора.
1. Выберите **Использовать текущий пароль устройства и адрес электронной почты** (Using current device password and email info).



Этот флажок установлен по умолчанию.

Рис 1–9 Применение настроек устройства

Enter Password

1 ☒ Using current device password and email info.

2 Next

2. Нажмите **Далее** (Next).

- Введение пароля и адреса электронной почты вручную.

1. Снимите флажок **Использовать текущий пароль устройства и адрес электронной почты** (Using current device password and email info).

Рис. 1–10 Установка пароля

Enter Password

1 ☐ Using current device password and email info.

2

User admin

Password

Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them.(please do not use special symbols like ' " ; : & )

Confirm Password

3 Next

2. Задайте пароль.

Таблица 1–3 Пароль

Параметр	Описание
Пользователь	Значение по умолчанию: <b>admin</b> . Изменить его нельзя.
Пароль	Новый пароль может содержать от 8 до 32 символов как минимум двух из следующих категорий: буквы, цифры и специальные знаки (кроме «'», «"», «;», «:» и «&»).
Подтверждение пароля	
	Введите надежный пароль в соответствии с индикатором шкалы надежности пароля.

3. Нажмите **Далее** (Next).

4. Введите адрес электронной почты и нажмите **Далее** (Next).

Рис. 1–11 Ввод адреса электронной почты

1 ☒ Email Address

To reset password, please input properly or update in time

Back 2 Next Skip

Шаг 5: Задайте IP-адрес камеры.

- Выберите **DHCP**, если используется DHCP-сервер.
- Выберите **Статический** (Static), а затем введите IP-адрес, маску подсети, шлюз по умолчанию и инкрементное значение.



Инкрементное значение устанавливается, если нужно изменить IP-адреса нескольких камер одновременно. При назначении IP-адресов для этих камер сетевой видеорегистратор будет постепенно добавлять значения в четвертую часть IP-адреса.

Рис. 1–12 Настройка IP-адреса

The screenshot shows a 'NETWORK' configuration window. At the top, it says 'Checked Device No.: 1'. Below this, there are two radio buttons: 'DHCP' (unselected) and 'STATIC' (selected). Under the 'STATIC' option, there are three input fields for 'IP Address', 'Subnet Mask', and 'Default Gateway', each containing a series of dots for digit entry. To the right of these fields is an 'Incremental Value' field with the number '1'. Below the input fields is a table with two columns: an index and a label. The first row has '1' in the index column and 'IP Address' in the label column. Below this, there are several empty rows. At the bottom of the window, there are three buttons: 'Back', 'Next', and 'Skip'.

1	IP Address
1	

Шаг 6: Нажмите **Далее** (Next).

Подождите 1–2 минуты до завершения инициализации.

Шаг 7: Нажмите **Готово** (Finished).

## 1.4.2Добавление IP-камеры по результату поиска

### Предварительные требования

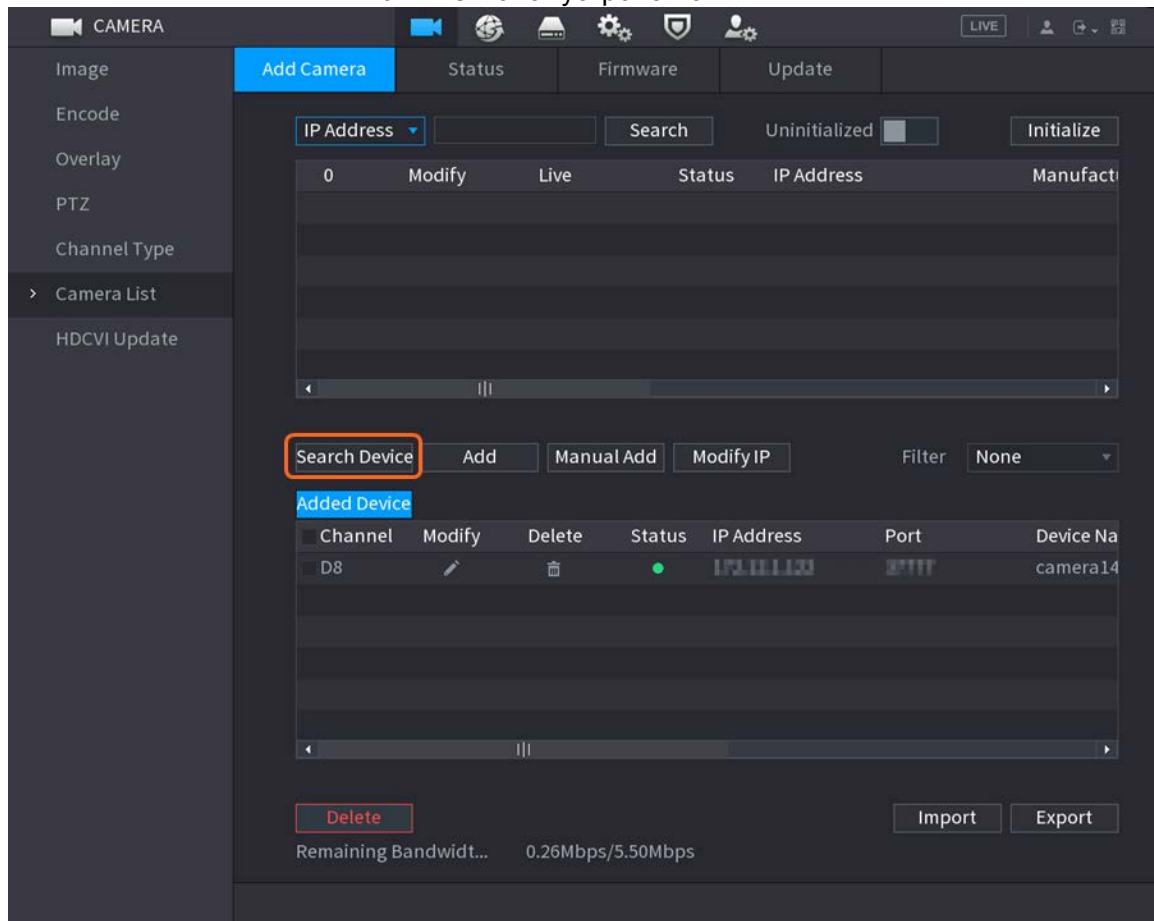
Убедитесь, что камеры, которые вы хотите добавить, уже инициализированы и подключены к требуемой сети.

### Процедура

Шаг 1: Выберите **Главное меню > КАМЕРА > Список камер > Добавить камеру** (Main Menu > Camera > Camera List > Add Camera).

Шаг 2: Нажмите **Поиск устройства** (Search Device).

Рис. 1–13 Поиск устройства



Шаг 3: Добавьте IP-камеры.

- Добавление двойным щелчком: дважды щелкните целевую камеру, чтобы добавить ее в список **Добавленные устройства** (Added Device).



По результатам поиска вы можете добавить только одну камеру за один раз.

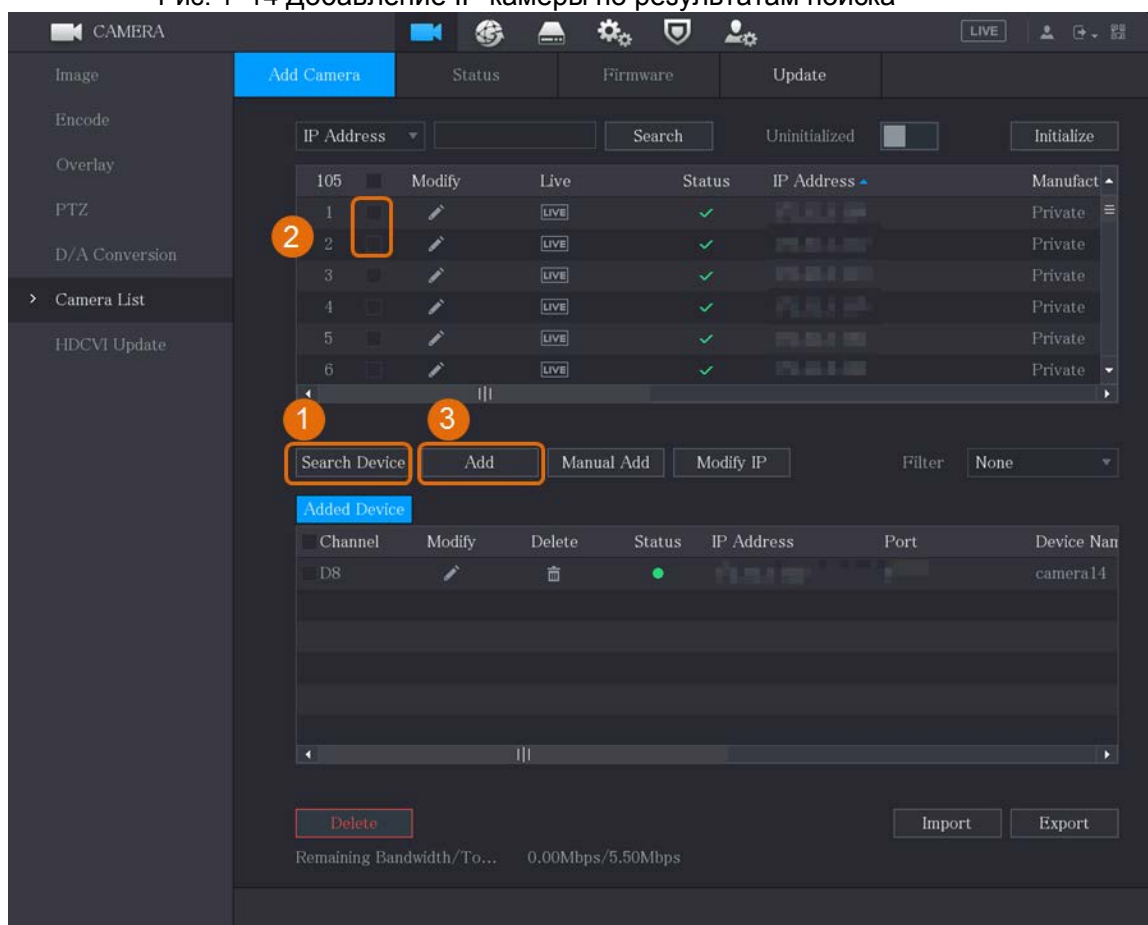
- Добавление с помощью флажка: установите флажок целевой камеры, а затем нажмите **Добавить** (Add), чтобы добавить ее в список **Добавленные устройства** (Added Device).





Вы можете установить несколько флажков и добавлять камеры группами.

Рис. 1–14 Добавление IP-камеры по результатам поиска



## Результат

- Если статус добавленной камеры зеленый (●), это означает, что камера корректно добавлена к NVR.
- Если статус добавленной камеры красный (●), это указывает на сбой соединения между камерой и NVR. Проверьте параметры камеры, такие как пароль, протокол и номер канала, а затем попробуйте добавить ее еще раз.

## 1.4.3Добавление IP-камеры вручную

Вы можете добавлять IP-камеры путем ввода IP-информации по одной за один раз.

### Предварительные требования

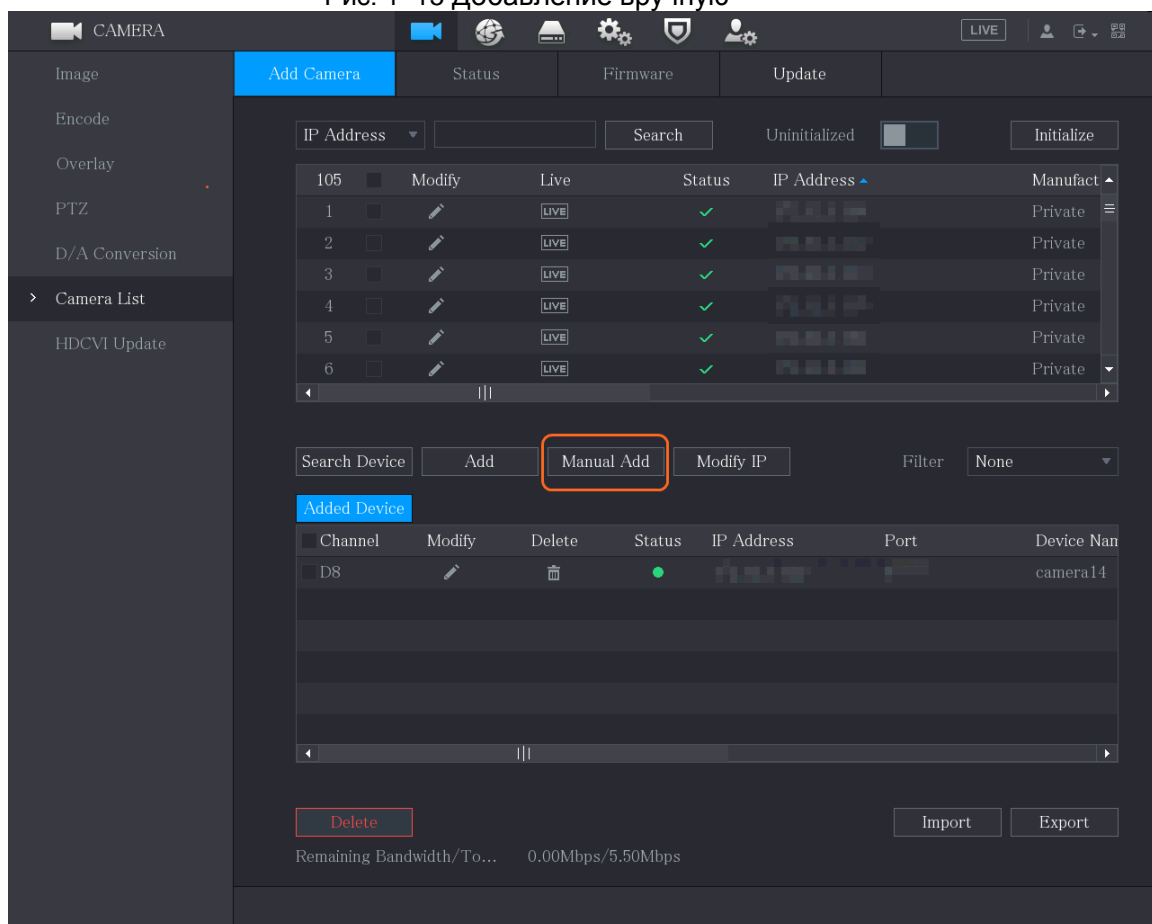
Убедитесь, что камеры, которые вы хотите добавить, уже инициализированы и подключены к требуемой сети.

### Процедура

Шаг 1: Выберите **Главное меню > КАМЕРА > Список камер > Добавить камеру** (Main Menu > Camera > Camera List > Add Camera).

Шаг 2: Нажмите **Добавить вручную** (Manual Add).

Рис. 1–15 Добавление вручную



**Шаг 3:** В диалоговом окне **Добавление вручную** (Manual Add) введите требуемые параметры.

Рис. 1–16 Ввод параметров для добавления вручную

Manual Add

Channel: D8

Manufacturer: ONVIF

IP Address: 192.168.0.0

RTSP Port: Self-adaptive

HTTP Port: 80

Username: admin

Password:

Total Channels: 1

Remote CH No.: D1

Decode Strategy: General

Encryption: ☐


☒ Auto ☐ TCP ☐ UDP ☐ MULTICAST

Connect Setting

OK Cancel

Таблица 1–4 Параметры для добавления вручную

Параметр	Описание
Канал	В раскрывающемся списке <b>Канал</b> (Channel) выберите канал NVR, который вы хотите использовать для подключения удаленного устройства.
Производитель	В раскрывающемся списке <b>Производитель</b> (Manufacturer) выберите производителя удаленного устройства.
IP-адрес	В поле <b>IP-адрес</b> (IP Address) введите IP-адрес IP-камеры.  Измените значение адреса по умолчанию (192.168.0.0), к которому система не может подключиться.
Порт RTSP	Значение по умолчанию: 554. При необходимости вы можете изменить значение.
Порт HTTP	Значение по умолчанию: 80. При необходимости вы можете изменить значение.  Если вы вводите другое значение, например 70, тогда вы должны ввести 70 после IP-адреса при входе в NVR через браузер.
Порт TCP	Значение по умолчанию: 37777. При необходимости вы можете изменить значение.
Имя пользователя	Введите имя пользователя удаленного устройства.
Пароль	Введите пароль пользователя удаленного устройства.
Номер удаленного канала.	Введите номер канала удаленного устройства, которое вы хотите добавить.

Параметр	Описание
Стратегия декодирования	В списке <b>Стратегия декодирования</b> (Decoder Strategy) выберите <b>По умолчанию</b> , <b>В реальном времени</b> или <b>Произвольно</b> (Default, Realtime или Fluent) по мере необходимости.
Тип протокола	<ul style="list-style-type: none"> <li>Если IP-камера добавляется по закрытому протоколу, выберите <b>TCP</b>.</li> <li>Если IP-камера добавляется по протоколу ONVIF, выберите <b>Авто</b>, <b>TCP</b>, <b>UDP</b> или <b>МУЛЬТИКАСТ</b> (Auto, TCP, UDP или MULTICAST).</li> <li>Если IP-камера добавляется по протоколам других производителей, выберите <b>TCP</b> или <b>UDP</b>.</li> </ul>
Шифрование	<p>Если IP-камера добавляется по протоколу ONVIF, установка флажка <b>Шифрование</b> (Encryption) обеспечит шифрование передаваемых данных.</p>  <p>Чтобы использовать эту функцию, необходимо включить режим <b>HTTPS</b> для удаленной IP-камеры.</p>

Шаг 4Нажмите **ОК**.

## 1.5 Настройка расписания хранения записанного видео

По умолчанию все камеры непрерывно записывают видео 24 часа в сутки. При необходимости вы можете изменить эти настройки.



Вы также можете настроить расписание хранения в мастере запуска.

Процедура

Шаг 1: Выберите **Главное меню > ХРАНИЛИЩЕ > Расписание > Запись** (Main Menu > STORAGE > Schedule > Record).


Рис. 1–17 Расписание записи



Шаг 2: Настройте параметры.


Таблица 1–5 Параметры записи

Параметр	Описание
Канал	В раскрывающемся списке <b>Канал</b> (Channel) выберите канал, для которого нужно изменить настройки видеозаписи.
Предварительная запись	В поле <b>Предварительная запись</b> (Pre-record) установите время для съемки дополнительного видео перед событием, чтобы обеспечить контекст для записи. Диапазон значений: от 0 до 30 с.

Параметр	Описание
Резервирование	<p>Эта функция позволяет выбрать один из жестких дисков в качестве резервного для сохранения записанных файлов на нескольких жестких дисках. В случае отказа основного жесткого диска вы можете найти резервную копию на резервном жестком диске.</p> <ul style="list-style-type: none"> <li>• Выберите <b>Главное меню &gt; ХРАНИЛИЩЕ &gt; Диспетчер дисков</b> (Main Menu &gt; STORAGE &gt; Disk Manager), а затем назначьте жесткий диск в качестве резервного.</li> <li>• Выберите <b>Главное меню &gt; ХРАНИЛИЩЕ &gt; Расписание &gt; Запись</b> (Main Menu &gt; STORAGE &gt; Schedule &gt; Record), а затем установите флажок <b>Резервирование</b> (Redundancy). <ul style="list-style-type: none"> <li>◇ Если выбранный канал не записывается, функция резервирования вступит в силу при следующей записи, независимо от того, установлен флажок или нет.</li> <li>◇ Если выбранный канал записывается, текущие записанные файлы будут упакованы, а затем начнется запись в соответствии с новым расписанием.</li> </ul> </li> </ul> <p></p> <ul style="list-style-type: none"> <li>• Данная функция доступна в выбранных моделях.</li> <li>• Резервный жесткий диск выполняет резервное копирование только видеозаписей, но не снимков.</li> </ul>
Типы событий	<p>Выбор флажков для типов событий.</p> <ul style="list-style-type: none"> <li>• <b>Общий (General):</b> общий тип записи означает, что NVR записывает все видео в течение указанного периода времени. Общий тип записи обозначается зеленым цветом.</li> <li>• <b>Движение (Motion):</b> тип записи при обнаружении движения означает, что видеорегистратор записывает видео только при срабатывании датчика движения. Тип записи при обнаружении движения обозначается желтым цветом.</li> <li>• <b>Тревога (Alarm):</b> тип записи по тревоге означает, что NVR записывает видео при срабатывании сигнализации. Тип записи по тревоге отображается красным цветом.</li> <li>• <b>M&amp;A:</b> тип записи M&amp;A объединяет запись при обнаружении движения и запись по сигналу тревоги. Устройство записывает видео при срабатывании датчика движения или по любому сигналу тревоги. Тип записи M&amp;A обозначается оранжевым цветом.</li> <li>• <b>Интеллектуальный (Intelligent):</b> интеллектуальный тип записи означает, что NVR записывает видео при срабатывании системы интеллектуального обнаружения. Интеллектуальный тип записи обозначается синим цветом.</li> <li>• <b>POS:</b> тип записи POS означает, что NVR записывает видео, когда для оплаты используется кассовый автомат. Тип записи POS обозначается фиолетовым цветом.</li> </ul>

Параметр	Описание
Период (Period)	Определяет период, в течение которого заданный режим записи активен. Система активирует тревогу только в определенный период.
Копировать (Copy to)	Вы можете нажать <b>Копировать</b> (Copy to), чтобы скопировать настройки для других каналов.

Шаг 3: Составьте расписание методом рисования или редактирования.

- Рисование: нажав и удерживая левую кнопку мыши, перемещайте мышь, чтобы нарисовать период.
- Редактирование: нажмите , чтобы задать период, а затем нажмите **ОК**.

Шаг 4: Нажмите кнопку **Применить** (Apply).



Настроенное расписание записи может вступить в силу только при включенной функции автоматической записи. Для получения дополнительной информации о включении функции автоматической записи см. Руководство пользователя.

## 1.6 Настройка параметров P2P

Чтобы подключить смартфон к NVR для управления, вы можете использовать QR-код.



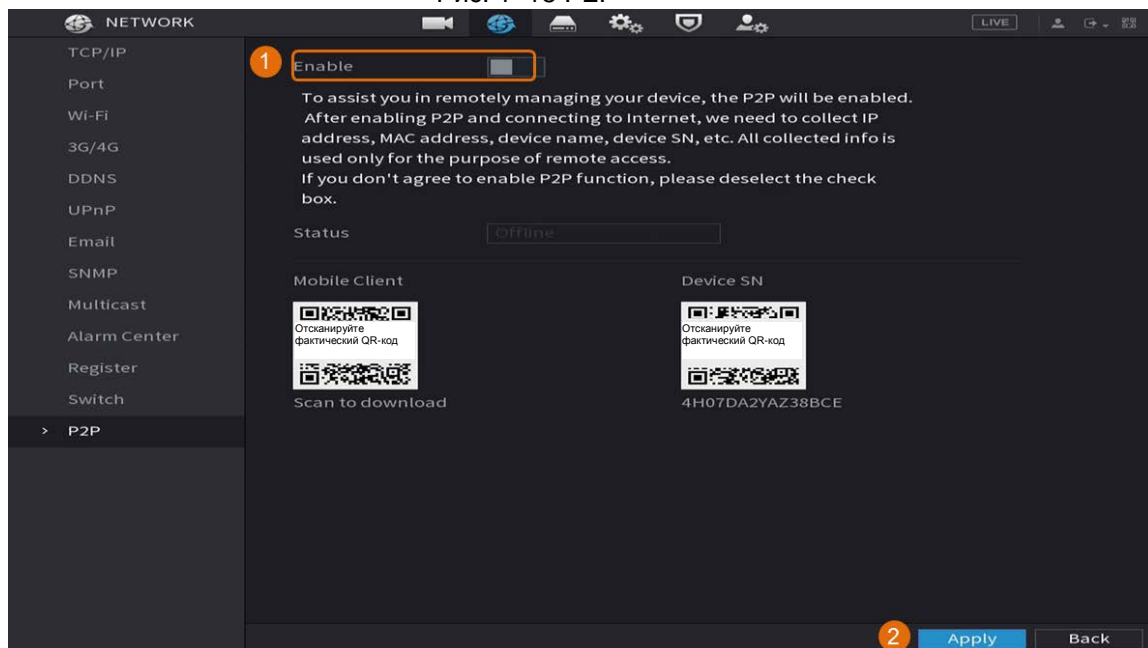
Убедитесь, что NVR подключен к Интернету. Если это так, тогда в поле **Статус** (Status) интерфейса P2P отображается **Онлайн** (Online).

### 1.6.1 Включение функции P2P

Вам необходимо войти в интерфейс P2P, чтобы включить функцию P2P, и отсканировать QR-код, чтобы загрузить приложение для смартфона.

Шаг 1: Выберите **Главное меню** > **СЕТЬ** > **P2P** (Main Menu > NETWORK > P2P).

Рис. 1–18 P2P




Шаг 2: Чтобы включить функцию P2P, нажмите **Включить** (Enable).

Шаг 3: Нажмите кнопку **Применить** (Apply)

## 1.6.2 Добавление сетевого видеорегистратора в клиентскую программу смартфона

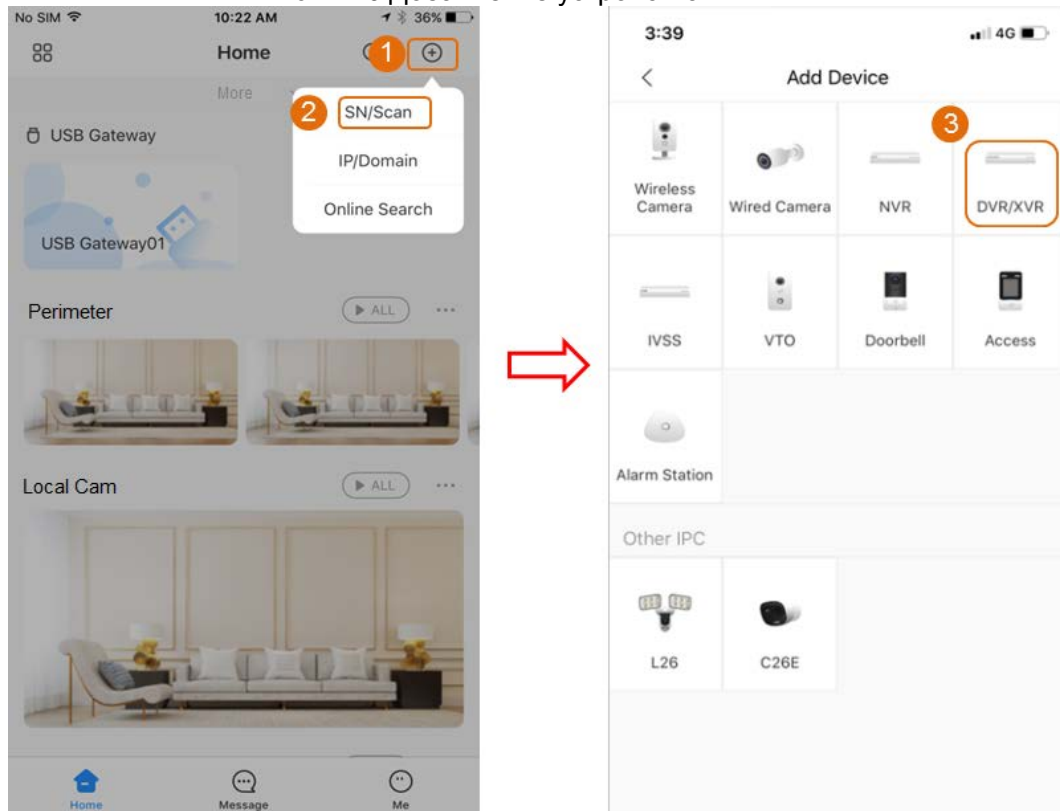
В этом разделе в качестве примера управления со смартфона рассматривается добавление сетевого видеорегистратора в клиентскую программу смартфона.

Шаг 1: Откройте приложение и нажмите .

Шаг 2: Выберите **Серийный №/сканирование** (SN/Scan).

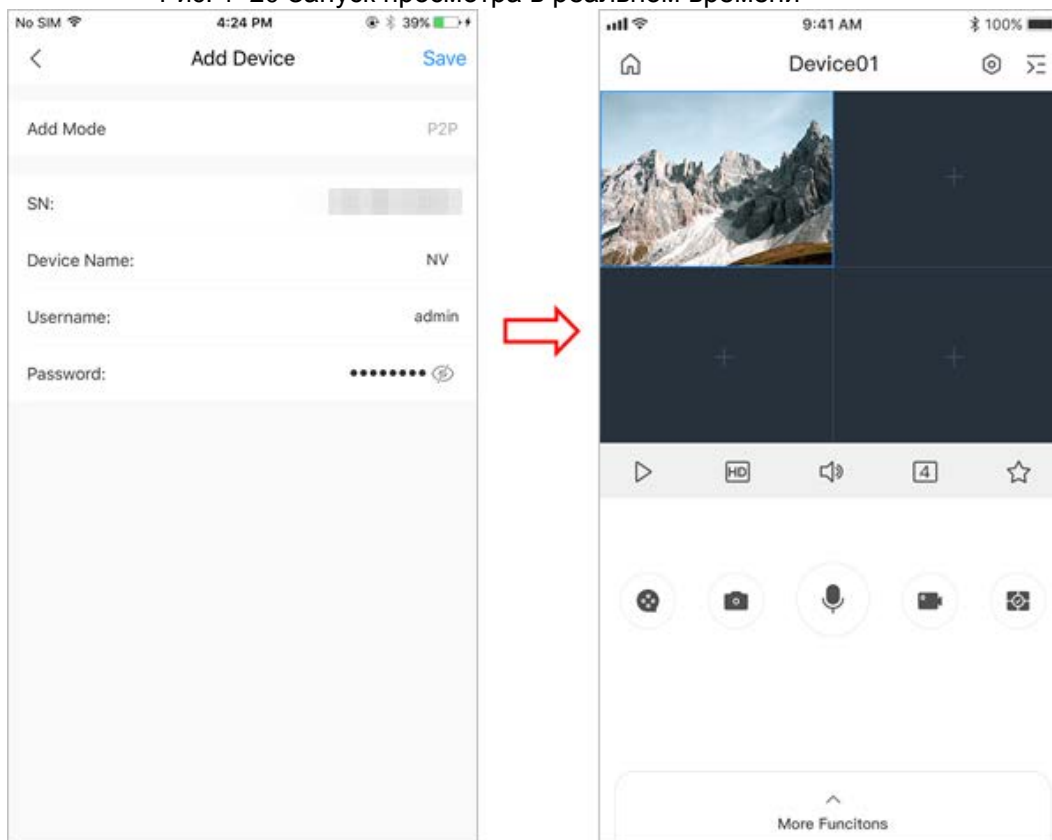


Рис. 1–19 Добавление устройства



Шаг 3: Выберите устройство, введите имя и пароль для NVR, а затем нажмите **Сохранить** (Save).

Рис. 1–20 Запуск просмотра в реальном времени



## 1.7 Интеллектуальное обнаружение движения

В этом разделе описано, как настроить функцию интеллектуального обнаружения движения (SMD).

### Исходная информация

Функция интеллектуального обнаружения движения (SMD) идеально подходит для мониторинга малых населенных пунктов, где требуется оповещение о движении людей или транспортных средств в любом месте сцены без установки правил и рисования линий.

### Процедура

Шаг 1: Выберите **Главное меню > AI > Параметры > SMD** (Main Menu > AI > Parameters > SMD).

Рис. 1–21 SMD

Channel: D1

Enable: ☐

Sensitivity: Medium

Effective Target: ☐ Human ☐ Motor Vehicle

Schedule:

Alarm-out Port:

☐ Show Message ☐ Report Alarm ☐ Send Email

☐ Record Channel:

☐ PTZ Linkage:

☐ Tour:

☐ Buzzer ☐ Log

☐ Alarm Tone: None

Anti-Dither: 0 sec.

Post-Alarm: 0 sec.

Post-Record: 10 sec.






☐ Picture Storage



SMD linkage configuration synchronizes with MD linkage configuration.

**Шаг 2:** Выберите и включите канал, а затем настройте параметры.

Таблица 1–6

Параметр	Описание
Чувствительность	Чем выше это значение, тем больше вероятность активации тревоги. Но в то же время повышается вероятность ложных тревог. Рекомендуется использовать значение по умолчанию.
Эффективная цель	Выберите человека, транспортное средство или обе эти цели.
Расписание	Настройте период, после чего в заданном временном интервале соответствующий элемент конфигурации будет связан для запуска сигнала тревоги.
Сглаживание колебаний	Указывает время, прошедшее с конца обнаружения движения до конца действия привязки сигнализации. Диапазон времени составляет от 0 до 600 сек.
Порт тревожного выхода	Порт тревожного выхода предназначен для подключения устройств сигнализации (таких как фары, сирены и т. д.). При возникновении тревоги NVR передает сигнал тревоги на устройство сигнализации.
Последующая тревога	Когда сигнал тревоги прекращается, тревога продлевается на заданный период времени. Диапазон времени: от 0 до 300 сек.
Показать сообщение	Установите этот флажок, чтобы включить всплывающее сообщение на локальном хосте-компьютере.

Параметр	Описание
Отчет о тревогах	<p>Установите этот флажок. При возникновении тревоги NVR передает сигнал тревоги в сеть (в том числе и в центр оповещения).</p>  <ul style="list-style-type: none"> <li>Данная функция доступна в выбранных моделях.</li> <li>Сначала нужно настроить функцию центра оповещения.</li> </ul>
Отправка писем	<p>Установите этот флажок. При возникновении тревоги NVR отправляет электронное письмо на заданный для уведомления адрес пользователя.</p>  <p>Сначала нужно задать адрес электронной почты.</p>
Запись канала	<p>Установите флажок и выберите необходимый канал записи (можно выбрать несколько вариантов). При возникновении тревоги NVR активирует канал для записи.</p>  <p>Сначала необходимо включить функции интеллектуальной и автоматической записи.</p>
Последующая запись	<p>После окончания тревоги запись продолжается в течение заданного периода времени. Диапазон времени: от 10 до 300 сек.</p>
Связь PTZ	<p>Установите флажок и нажмите кнопку настройки, чтобы выбрать канал и действие PTZ. При возникновении тревоги устройство NVR связывает канал, чтобы выполнить соответствующее действие PTZ. Например, вы можете активировать PTZ в канале 1, чтобы повернуть камеру в заданную точку X.</p>  <ul style="list-style-type: none"> <li>Сигнализация растяжки поддерживает только активацию PTZ для заданной точки.</li> <li>Сначала нужно задать соответствующие действия PTZ.</li> </ul>
Обзор	<p>Установите флажок и выберите канал для обзора. При возникновении тревоги на локальном интерфейсе NVR отображается экран выбранного канала.</p>  <ul style="list-style-type: none"> <li>Сначала необходимо установить интервал времени и режим обзора.</li> <li>После завершения обзора интерфейс предварительного просмотра снова переходит в режим разделенного экрана, который был установлен до начала обзора.</li> </ul>

Параметр	Описание
Хранилище изображений	<p>Установите флажок <b>Снимок</b> (Snapshot), чтобы сделать снимок с выбранного канала.</p> <p></p> <p>Чтобы использовать эту функцию, выберите <b>Главное меню &gt; КАМЕРА &gt; Кодирование &gt; Снимок</b> (Main Menu &gt; CAMERA&gt; Encode &gt; Snapshot), а затем выберите <b>Событие</b> (Event) в списке <b>Тип</b> (Type).</p>
Зуммер	<p>Установите это флажок, чтобы активировать зуммер на устройстве при возникновении тревоги.</p>
Звуковой сигнал тревоги	<p>Установите этот флажок, а затем выберите соответствующий звуковой файл из раскрывающегося списка. Система будет воспроизводить этот звуковой файл при возникновении тревоги.</p> <p></p> <p>Сначала нужно добавить аудиофайл.</p>

Шаг 3: Нажмите кнопку **Применить** (Apply).

## 1.8 Просмотр в реальном времени


После выполнения входа система переключается в режим многоканального просмотра в реальном времени. Вы можете просматривать видео для мониторинга каждого канала. Обратите внимание, что количество отображаемых окон зависит от конкретной модели. Чтобы перейти на экран просмотра в реальном времени из других интерфейсов, нажмите  в верхнем правом углу экрана.

Рис. 1–22 Просмотр в реальном времени







## Экран просмотра в реальном времени

Вы можете просматривать видео в реальном времени с подключенных камер через каждый канал на экране.

- По умолчанию системное время, название и номер канала отображаются в окне каждого канала. Чтобы настроить этот параметр, выберите **Главное меню > КАМЕРА > Наложение > Наложение** (Main Menu > CAMERA > Overlay > Overlay).
- На рисунке в нижнем правом углу показан номер канала. Если позиция или название канала изменяется, вы можете узнать номер канала на этом рисунке, а затем выполнять такие операции, как запрос записи и воспроизведения.

Описание значков, отображаемых в каждом канале, приведено в Таблица 1–7.

Таблица 1–7 Описание значков

Значок	Описание
	Записывается видео.
	На сцене обнаружено движение.
	Обнаружена потеря видеосигнала.
	Мониторинг каналов заблокирован.

## 1.9 Запись в процессе воспроизведения

Для воспроизведения записи вы можете выбрать **Главное меню > Воспроизведение** (Main Menu > Playback) или щелкнуть правой кнопкой мыши в интерфейсе просмотра в реальном времени и выбрать **Поиск** (Search).

Рис. 1–23 Основной интерфейс воспроизведения




Для получения дополнительной информации об использовании основного интерфейса воспроизведения см. *Руководство пользователя*.



## Мгновенное воспроизведение

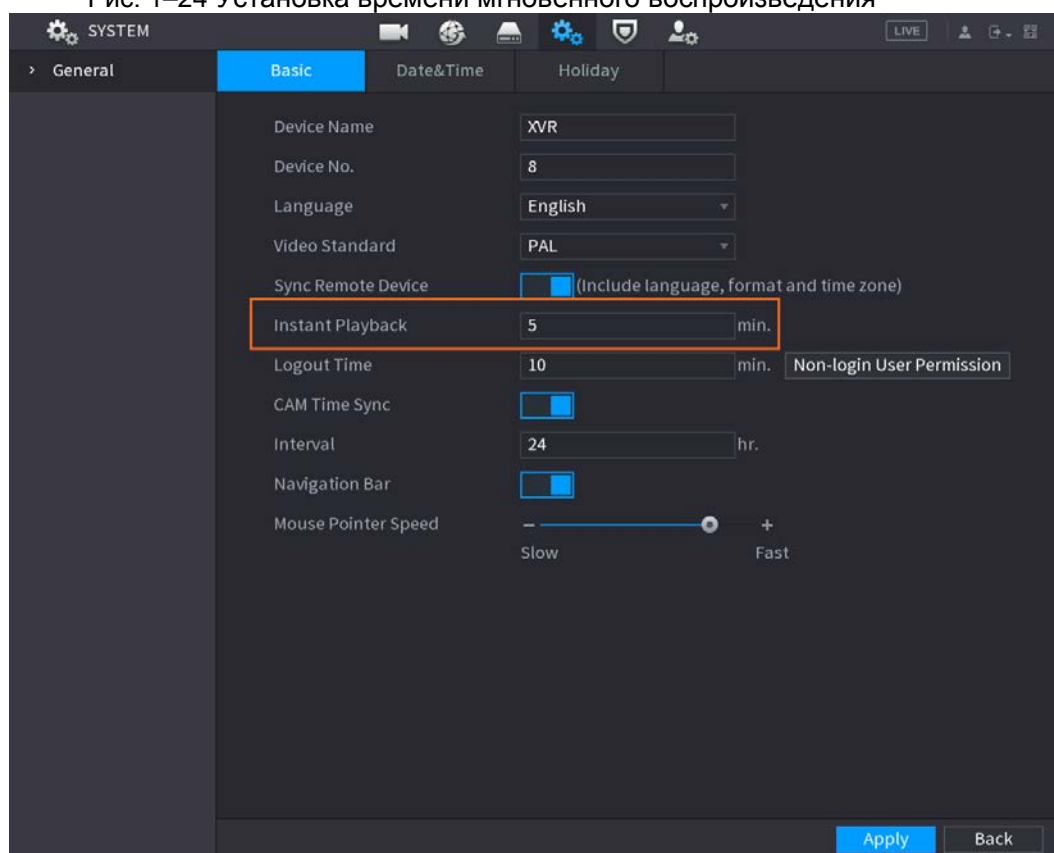
Вы можете воспроизвести видеозапись за предыдущие 5–60 минут.

После нажатия  открывается интерфейс воспроизведения. Мгновенное воспроизведение имеет следующие функции:

- Переместите ползунок, чтобы выбрать время для начала воспроизведения.
- Запуск воспроизведения, пауза и остановка воспроизведения.
- Информация, такая как имя канала и значок состояния записи, скрыта во время мгновенного воспроизведения и не будет отображаться до выхода из этого режима.
- Во время воспроизведения переключение разделения экрана не допускается.

Чтобы изменить время воспроизведения, выберите **Главное меню > СИСТЕМА > Общие > Базовые** (Main Menu > SYSTEM > General > Basic) и в поле **Мгновенное воспроизведение** (Instant Playback) введите требуемое время воспроизведения.

Рис. 1–24 Установка времени мгновенного воспроизведения



## Воспроизведение с интеллектуальным поиском

Во время воспроизведения вы можете проанализировать определенную область, чтобы определить, произошло ли какое-либо событие при обнаружении движения. Система будет отображать изображения с событиями при обнаружении движения в записанном видео.



Эта функция доступна только для устройств некоторых серий.

Чтобы использовать функцию интеллектуального поиска, необходимо включить обнаружение движения для канала, выбрав **Главное меню > ТРЕВОГА > Обнаружение видео > Обнаружение движения** (Main Menu > ALARM > Video Detection > Motion Detection).

## 2 Вход в веб-интерфейс

Интернет требуется для работы большинства функций в локальном графическом интерфейсе. Вы можете войти в сеть для управления NVR.



В интерфейсах разных моделей могут быть небольшие различия. Следующие рисунки приведены только для справки. Преимущественную силу имеют характеристики и параметры фактического устройства.


### Процедура

Шаг 1: Откройте браузер и введите IP-адрес сетевого видеорегистратора, а затем нажмите клавишу Enter.

Шаг 2: Введите имя пользователя и пароль.

Рисунок 2-1 Вход в систему



- Имя аккаунта администратора по умолчанию: **admin**. Пароль используется тот, который был задан при начальных настройках. Для обеспечения безопасности аккаунта рекомендуется хранить пароль надлежащим образом и регулярно его менять.
- Нажмите , чтобы отобразить пароль.

Шаг 3: Нажмите **Вход** (Login).



# Приложение 1 Рекомендации по кибербезопасности

Кибербезопасность – это больше, чем просто модное слово: это то, что относится к каждому устройству, подключенному к Интернету. Сетевое видеонаблюдение не застраховано от киберрисков, но принятие основных мер по защите сетей и сетевых устройств делает оборудование менее уязвимыми для атак. Ниже приведены советы и рекомендации по созданию более защищенной системы безопасности.

## **Обязательные действия, которые необходимо предпринять для обеспечения защиты сети основного оборудования:**

### **1. Используйте надежные пароли**

Ознакомьтесь со следующими советами по установке паролей:

- Пароль должен содержать не менее 8 символов.
- Используйте как минимум два типа символов, включая буквы верхнего и нижнего регистра, числа и специальные знаки.
- Не используйте в качестве пароля имя аккаунта в обратном порядке.
- Не используйте последовательные символы, такие как 123, abc и т. д.
- Не используйте одинаковые символы, например 111, aaa и т. д.

### **2. Своевременно обновляйте прошивку и клиентское программное обеспечение**

- В соответствии со стандартной процедурой, принятой в ИТ-индустрии, мы рекомендуем обновлять прошивку вашего оборудования (NVR, DVR, IP-камер и т. д.), чтобы гарантировать, что в системе установлены последние исправления, обеспечивающие безопасность. Когда оборудование подключено к общедоступной сети, рекомендуется включить функцию **автоматической проверки обновлений** (auto-check for updates), чтобы своевременно получать информацию об обновлениях прошивки, выпущенных производителем.
- Мы предлагаем вам загрузить и использовать последнюю версию клиентского программного обеспечения.

## **Рекомендации по повышению сетевой безопасности вашего оборудования:**

### **1. Физическая защита**

Мы рекомендуем обеспечить физическую защиту оборудования, особенно запоминающих устройств. Например, разместите оборудование в специальном компьютерном зале или в шкафу и обеспечьте хорошо продуманный контроль доступа и управление ключами, чтобы предотвратить несанкционированный доступ персонала к физическому оборудованию с целью его повреждения или подключения съемных устройств (таких как флэш-накопители) через USB порт, последовательный порт и т. д.

### **2. Регулярно меняйте пароль**

Мы рекомендуем регулярно менять пароли, чтобы снизить риск их подбора или взлома.

### **3. Своевременно вводите и обновляйте информацию для сброса паролей**

Оборудование поддерживает функцию сброса пароля. Своевременно укажите необходимую информацию для сброса пароля, включая адрес электронной почты конечного пользователя и контрольные вопросы для защиты пароля. Если информация изменится, обновите ее вовремя. При введении контрольных вопросов для защиты пароля рекомендуется не использовать те, которые легко угадать.

4. Включите блокировку аккаунта  
Функция блокировки аккаунта включена по умолчанию, и мы рекомендуем оставить ее включенной, чтобы гарантировать безопасность аккаунта. Если злоумышленник несколько раз попытается войти в систему с неправильным паролем, соответствующий аккаунт и исходный IP-адрес будут заблокированы.
5. Измените порты HTTP и других служб, используемые по умолчанию  
Чтобы снизить риск того, что посторонние смогут угадать, какие порты вы используете, мы рекомендуем изменить номера портов HTTP и других служб, используемые по умолчанию, на любые другие из диапазона от 1024 до 65535.
6. Включите HTTPS  
Мы предлагаем включить HTTPS, чтобы пользоваться веб-службой через безопасный канал связи.
7. Активируйте белый список  
Мы предлагаем активировать белый список, чтобы предоставить доступ к системе только с указанных IP-адресов. При этом не забудьте добавить IP-адрес своего компьютера и IP-адреса вспомогательного оборудования в белый список.
8. Присоедините MAC-адрес  
Мы рекомендуем привязать IP-адрес и MAC-адрес шлюза к оборудованию, чтобы снизить риск спуфинга ARP.
9. Грамотно назначайте аккаунты и полномочия  
Грамотно добавляйте пользователей и назначайте им минимальный набор полномочий в соответствии с требованиями бизнеса и администрирования.
10. Отключите ненужные службы и выберите безопасные режимы  
Если в этом нет необходимости, рекомендуется отключить некоторые службы, такие как SNMP, SMTP, UPnP и т. д., чтобы снизить риски.

При необходимости настоятельно рекомендуется использовать безопасные режимы, включая нижеследующие:

- SNMP: Выберите SNMP v3 и установите надежные пароли шифрования и аутентификации.
  - SMTP: Выберите TLS для доступа к почтовому серверу.
  - FTP: Выберите SFTP и установите надежные пароли.
  - Точка доступа (AP): Выберите режим шифрования WPA2-PSK и установите надежные пароли.
11. Используйте шифрование для передачи аудио и видео  
Если содержимое ваших аудио- и видеоданных очень важно или конфиденциально, рекомендуется использовать функцию зашифрованной передачи, чтобы снизить риск перехвата этих данных во время передачи.  
Напоминание: шифрование вызовет некоторое снижение скорости передачи.
  12. Выполняйте проверки безопасности
    - Проверяйте сетевых пользователей: мы рекомендуем регулярно проверять сетевых пользователей, чтобы выяснить, не вошел ли кто-либо в систему NVR без авторизации.
    - Проверяйте журнал оборудования: просматривая журналы, вы можете узнать IP-адреса, которые использовались для входа в ваши устройства, и их основные операции.

13. Используйте сетевой журнал

Из-за ограниченного объема памяти оборудования объем данных, сохраняемых в журнале, также ограничен. Если вам нужно хранить журнал в течение длительного времени, рекомендуется включить функцию сетевого журнала, чтобы гарантировать отслеживание информации путем синхронной передачи критических данных на сервер сетевого журнала.

14. Создайте безопасную сетевую среду

Чтобы повысить уровень безопасности оборудования и снизить потенциальные киберриски, рекомендуется принять перечисленные ниже меры.

- Отключите функцию сопоставления портов маршрутизатора, чтобы избежать прямого доступа к устройствам интрасети из внешней сети.
- Сеть должна быть разделена и изолирована в соответствии с реальными сетевыми потребностями. Если между двумя подсетями не требуется обмениваться данными, рекомендуется использовать VLAN, сетевой стандарт GARP и другие технологии для разделения сети, чтобы добиться эффекта сетевой изоляции.
- Выберите систему аутентификации доступа 802.1x, чтобы снизить риск несанкционированного доступа к частным сетям.

15. Рекомендуется включить брандмауэр вашего устройства или функции запрещенного и разрешенного списков, чтобы снизить риск атак на ваше устройство.