

УТВЕРЖДЕН
ЦРПА.2.00124.01.00 92-ЛУ

**СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ
«АССаД-Видео»**

Руководство администратора безопасности

ЦРПА.2.00124.01.00 92

Листов 34

Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

2024

АННОТАЦИЯ

Настоящее руководство администратора безопасности информации содержит сведения по настройке и сопровождению встроенных средств защиты информации от несанкционированного доступа специального программного обеспечения системы видеонаблюдения «АССаД-Видео» (далее — СПО «АССаД-Видео») ЦРПА.2.00124.01.00.

Руководство предназначено для администраторов безопасности информации, зарегистрированных в СПО «АССаД-Видео» как пользователи с ролью «Администратор безопасности».

Администраторы безопасности информации ответственны за защиту информации от несанкционированного доступа в системе «АССаД-Видео». Администраторы безопасности осуществляют управление разграничением доступа операторов и системных администраторов к функциям и данным, ведение паролей операторов и системных администраторов для входа в систему, тестирование СЗИ НСД и контроль данных аудита действий операторов и системных администраторов.

Работа с остальными функциями СПО «АССаД-Видео» описана в руководстве системного программиста ЦРПА.2.00124.01.00 32 и руководстве оператора ЦРПА.2.00124.01.00 34.

В настоящем руководстве приняты следующие сокращения:

АСФЗ	— автоматизированная система физической защиты;
АРМ	— автоматизированное рабочее место;
БД	— база данных;
ИБП	— источник бесперебойного питания;
НСД	— несанкционированный доступ;
ОС	— операционная система;
ЛВС	— локальная вычислительная сеть;
ПО	— программное обеспечение;
СЗИ	— средства защиты информации;
СКУД	— система управления и контроля доступом;
СОЭН	— система оптико-электронного наблюдения;
СПО	— специальное программное обеспечение;
ССОИ	— система сбора и обработки информации;
ТС	— технические средства.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ О СРЕДСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА	4
2 ОГРАНИЧЕНИЯ ИНТЕРФЕЙСА ОПЕРАТОРАМ	5
2.1 Общие сведения	5
2.2 Настройка ограниченного интерфейса на АРМ	5
3 РЕАЛИЗАЦИЯ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ	10
3.1 Организация доступа к программе	10
3.2 Контроль над действиями пользователей	11
3.3 Контроль доступа к оборудованию	12
4 КОНТРОЛЬ ЦЕЛОСТНОСТИ СЗИ	13
4.1 Общие сведения	13
4.2 Автоматический и автоматизированный контроль целостности файлов	13
4.3 Тестирование СЗИ	14
5 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ОПЕРАТОРОВ	16
5.1 Приложение Учетные записи	16
5.1.1 Управление ролями	17
5.1.2 Назначение ролей	20
5.1.3 Настройка параметров безопасности	20
5.1.4 Управление пользователями	22
6 НАСТРОЙКА ДОСТУПА К ЭКРАНАМ И КАНАЛАМ	24
7 РЕГИСТРАЦИЯ СОБЫТИЙ	26
8 УПРАВЛЕНИЕ ДОСТУПНОСТЬЮ ПРИЛОЖЕНИЙ В МЕНЮ М7	28
9 ЖУРНАЛЫ СОБЫТИЙ	30
10 СООБЩЕНИЯ АДМИНИСТРАТОРУ БЕЗОПАСНОСТИ	32
ПРИЛОЖЕНИЕ А ПОРЯДОК УСТРАНЕНИЯ НЕДОСТАТКОВ И УЯЗВИМОСТЕЙ И ДОВЕДЕНИЯ ОБНОВЛЕНИЙ ДО ПОТРЕБИТЕЛЕЙ	33

1 ОБЩИЕ СВЕДЕНИЯ О СРЕДСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Средства защиты от несанкционированного доступа к информации СПО «АССаД-Видео» включают:

- средства аутентификации операторов в СПО «АССаД-Видео»;
- средства управления доступом операторов к ресурсам «АССаД-Видео», реализованные с помощью ролей;
- средства регистрации событий, произошедших при работе СПО «АССаД-Видео»;
- средства обеспечения контроля целостности.

Средства защиты информации СПО «АССаД-Видео» объединены в платформу «М7».

В составе персонала АСФЗ должен быть назначен администратор безопасности, ответственный за ведение СЗИ НСД, загрузку и останов системы на компьютерах, её восстановление и тестирование. Для администратора безопасности должно быть выделено отдельное рабочее место (сервер, рабочая станция) для сопровождения СЗИ НСД и контроля безопасности системы.

Администраторы безопасности осуществляют настройку и сопровождение СЗИ НСД, включая управление разграничением доступа операторов и системных администраторов АСФЗ к функциям и данным, ведение паролей операторов и системных администраторов для входа в систему, тестирование СЗИ НСД и контроль данных аудита действий операторов и системных администраторов.

Установка и настройка СЗИ НСД осуществляется в следующем порядке:

- а) установка ОС «Astra Linux Special Edition» (версии 1.6 «Смоленск») согласно разделу 3 руководства системного программиста ЦРПА.2.00124.01.00 32;
- б) установка СПО «АССаД-Видео» согласно разделу 3 руководства системного программиста ЦРПА.2.00124.01.00 32;
- в) установка антивирусной программы согласно разделу 3 руководства системного программиста ЦРПА.2.00124.01.00 32 и документации антивирусной программы;
- г) настройка ограничений интерфейса пользователям на АРМ;
- д) регистрация сетевых узлов, серверов и видеорегистраторов в СПО «АССаД-Видео»;
- е) регистрация ролей и операторов в СПО «АССаД-Видео»;
- ж) конфигурация экранов в СПО «АССаД-Видео»;
- з) назначение прав доступа в СПО «АССаД-Видео»;
- и) проверка возможности входа операторов в систему с АРМ и соответствия экрана АРМ функционалу в рамках, предоставленных администратором безопасности прав и полномочий.

2 ОГРАНИЧЕНИЯ ИНТЕРФЕЙСА ОПЕРАТОРАМ

2.1 Общие сведения

На компьютерах системы операторам должен предоставляться ограниченный интерфейс системы в рамках, предоставленных администратором безопасности прав и полномочий, не позволяющий выполнять какие-либо программы и команды ОС.

Допускается операторам при входе в ОС на АРМ использовать одну учетную запись пользователя ОС (например, **algont**).

Регистрация всех операторов АРМ «АССаД-Видео» в ОС производится только под учетной записью пользователя **algont**.

Если во время установки ОС не был задан пароль суперпользователя **root**, необходимо его задать, выполнив следующие действия:

- выполнить вход в ОС под учетной записью пользователя, созданной при установке ОС;
- в консоли выполнить команду `sudo passwd root`;
- ввести новый пароль суперпользователя **root**;
- выбрать целостность – 63.

После установки СПО «АССаД-Видео» необходимо изменить пароль учетной записи ОС **algont** в соответствии с установленным порядком формирования и смены паролей.

Изменение пароля пользователя ОС выполняется следующим образом:

- войти в ОС под учетной записью пользователя **root**;
- в эмуляторе терминала выполнить команду установки пароля `passwd`, например, `passwd algont`;
- ввести новый пароль.

К паролям учетных записей **root** и **algont** должен применяться установленный порядок формирования и смены паролей, а также порядок ознакомления, обеспечивающие их конфиденциальность.

2.2 Настройка ограниченного интерфейса на АРМ

Для учетной записи **algont** должна быть выполнена настройка среды, не позволяющая оператору выполнять какие-либо программы и команды ОС. Данная настройка выполняется автоматически при установке СПО «АССаД-Видео» в режиме «Установка СПО рабочей станции».

Настройка конфигурации АРМ и ограничений интерфейса в процессе инсталляции выполняются с помощью скрипта <путь к распакованному дистрибутиву>/for-workstation/close_arm_1_6/install.sh, который вызывается в процессе установки программного обеспечения рабочего места оператора. Далее приведено содержимое скрипта `install.sh`:

```
#!/bin/bash
clear
SCRIPT_PATH=$(readlink -f $0)
CUR_DIR=`dirname $SCRIPT_PATH`
CHECKER_DIR="/opt/assad-video-checker"
. $CUR_DIR/progress.sh
. $CUR_DIR/data/arm-bin.astra/arm-launcher.cfg
DOMAIN="$ (hostname --domain) "
echo_bold() {
    tput bold
```

```

echo $1
tput sgr0
}
greeting() {
local cols=$(tput cols)
local G_MSG="* Настройка APM *"
local G_MSG_LEN=${#G_MSG}
local center=$((cols - $G_MSG_LEN))
local center=$((center / 2))
local tocenter=$(tput hpa $center)
local cnt=0;
tput bold
echo -n "${topleft}"
while [ $cnt -lt $G_MSG_LEN ]
do
echo -n "*"
let "cnt = cnt + 1"
done
echo
echo "${topleft}$G_MSG"
echo -n "${topleft}"
cnt=0
while [ $cnt -lt $G_MSG_LEN ]
do
echo -n "*"
let "cnt = cnt + 1"
done
echo
tput sgr0
}
create_algont() {
startProgress "Создание пользователя 'algont'"
USR_ALGONT=`cat /etc/passwd | grep algont`
[ "X$USR_ALGONT" != "X" ] || {
groupadd algont
useradd -m -g algont algont
usermod -p $(echo algont | openssl passwd -1 -stdin) algont
}
chage -M -1 algont
stopProgress
}
install_arm() {
startProgress "Настройка APM"
mkdir -p $CHECKER_DIR/bin
cp -rf $CUR_DIR/data/arm-bin.astra/* $CHECKER_DIR/bin/
chmod +x $CHECKER_DIR/bin/*.sh
$CUR_DIR/closeAstra/mountDVD.sh
if apt install openbox -y
then
echo ""
else
echo -e "\e[41mНе удалось установить Openbox\e[0m"
fi
# Disable kiosk for openbox
#mkdir -p /etc/fly-kiosk/algont
#cp -R $CUR_DIR/data/algont /etc/fly-kiosk/
stopProgress
}
final_close(){
if grep -q root:!/etc/shadow;
then
# echo 'root unconfigured'
PASS=$(whiptail --inputbox "Введите пароль для пользователя root" 8
78 "12345678" --title "Закрытие среды оператора" 3>&1 1>&2 2>&3)

```

```

    echo -e "$PASS\n$PASS" | passwd root
else
    echo 'root configured. skipping'
fi
# remove root access from algont user
deluser algont astra-admin
# autologin
echo "Выполняется отключение Режима Мандатного Контроля Целостности"
astra-mic-control disable
echo "Отключение выполнено"
echo "Настройка автологина пользователя"
# Enable Openbox
cp -b $CUR_DIR/closeAstra/files/menu.xml /etc/xdg/openbox
PASSWORD=$(echo YWxnb250Cg== | base64 --decode)
echo -e "$PASSWORD\n$PASSWORD\n" | passwd algont
sed -i -i 's/#AutoLoginPass=secret!/AutoLoginPass='$PASSWORD'/g'
/etc/X11/fly-dm/fly-dmrc
sed -i 's/.*AutoLoginUser.*/AutoLoginUser=algont/g' /etc/X11/fly-dm/fly-
dmrc
# disabling screen lock
echo "Отключение сна и гибернации"
echo "/usr/bin/xset -dpms" >> /etc/X11/fly-dm/Xsetup
sed -i 's/ScreenSaverDelay=600/ScreenSaverDelay=0/g' /usr/share/fly-
wm/theme/*themerc*
sed -i 's/LockerDpmsOffTimeout=600/LockerDpmsOffTimeout=0/g'
/usr/share/fly-wm/theme/*themerc*
sed -i 's/ScreenSaverDelay=600/ScreenSaverDelay=0/g'
~/.fly/theme/*themerc*
sed -i 's/LockerDpmsOffTimeout=600/LockerDpmsOffTimeout=0/g'
~/.fly/theme/*themerc*
mkdir -p /etc/X11/xorg.conf.d
#cp files/10-monitor.conf /etc/X11/xorg.conf.d/
}

first_checking() {
if [ "$(id -u)" != "0" ]; then
    echo "Данный скрипт должен быть запущен с root-правами"
    exit 1
fi
MONITORS=$(whiptail --title "Сколько мониторов APM?" --checklist \
"Сколько мониторов подключено к APM?" 15 60 4 \
"1" "Один монитор" OFF \
"2" "Два монитора" OFF \
"3" "Три монитора" OFF \
"4" "Четыре монитора" OFF 3>&1 1>&2 2>&3)

exitstatus=$?
if [ $exitstatus = 0 ]; then {
    sed -i 's/.*MONITOR_COUNT.*/MONITOR_COUNT='$MONITORS'/'
$CUR_DIR/data/arm-bin.astra/arm-launcher.cfg
}
}
else {
    echo "Выбор не сделан. Выход"
    exit 1
}
fi
}

set_startpage() {
    START_PAGE_VARIABLE="START_PAGE"
    # sed -i -e "s#$START_PAGE_VARIABLE#$START_PAGE#g"
$CHECKER_DIR/bin/arm-launcher
    sed -i -e
"s#MONITOR1_URL=\"http://video.algont\"#MONITOR1_URL=\"$START_PAGE\"#g"
$CHECKER_DIR/bin/arm-launcher.cfg

```

```

    sed -i -e
    "s#MONITOR2_URL=\"http://video.algont\"#MONITOR2_URL=\"\${START_PAGE}\"#g"
    \$CHECKER_DIR/bin/arm-launcher.cfg
    sed -i -e
    "s#MONITOR3_URL=\"http://video.algont\"#MONITOR3_URL=\"\${START_PAGE}\"#g"
    \$CHECKER_DIR/bin/arm-launcher.cfg
    sed -i -e
    "s#MONITOR4_URL=\"http://video.algont\"#MONITOR4_URL=\"\${START_PAGE}\"#g"
    \$CHECKER_DIR/bin/arm-launcher.cfg
  }
  first_checking
  final_close

START_PAGE=$(whiptail --inputbox "Введите стартовую страницу" 8 78
"http://video.\${DOMAIN}" 3>&1 1>&2 2>&3)
greeting
echo
echo_bold "Начало установки"
create_algont
install_arm
set_startpage
cd \$CUR_DIR/closeAstra
./close.sh
echo_bold "Установка завершена"

```

После установки СПО «АССаД-Видео» и перезагрузки АРМ выполняется автоматический запуск веб-браузера Firefox и переход к странице авторизации пользователя СПО «АССаД-Видео». Оператор АРМ проходит авторизацию с использованием личного логина и пароля, после которой ему предоставляется интерфейс в рамках прав доступа, предоставленных администратором безопасности.

Автоматический запуск веб-браузера Firefox обеспечивается с помощью скрипта arm-launcher, добавленного в автозагрузку. Данный скрипт также выполняет запрет горячих клавиш:

```

# Swap ctrl and caps
xmodmap -e 'remove Lock = Caps_Lock'
xmodmap -e 'remove Control = Control_L'
xmodmap -e 'keysym Control_L = Caps_Lock'
xmodmap -e 'keysym Caps_Lock = Control_L'
xmodmap -e 'add Lock = Caps_Lock'
xmodmap -e 'add Control = Control_L'
# Disabling keys
xmodmap -e 'keycode 67=NoSymbol' #F1
xmodmap -e 'keycode 68=NoSymbol' #F2
xmodmap -e 'keycode 69=NoSymbol' #F3
xmodmap -e 'keycode 70=NoSymbol' #F4
xmodmap -e 'keycode 72=NoSymbol' #F6
xmodmap -e 'keycode 73=NoSymbol' #F7
xmodmap -e 'keycode 74=NoSymbol' #F8
xmodmap -e 'keycode 75=NoSymbol' #F9
xmodmap -e 'keycode 76=NoSymbol' #F10
xmodmap -e 'keycode 96=NoSymbol' #F12
xmodmap -e 'keycode 37=NoSymbol' #LCtrl
xmodmap -e 'keycode 105=NoSymbol' #Rctrl

```

В процессе эксплуатации администратор безопасности может с помощью скриптов из каталога [путь к распакованному дистрибутиву]/for-workstation/close_arm_1_6/closeAstra/ поставочного диска (см. табл. 1) выполнить снятие и обратную установку ограничений интерфейса оператора. Запуск скриптов выполняется на АРМ под учетной записью суперпользователя root.

Таблица 1 — Скрипты настройки среды на АРМ

Название скрипта	Описание
close.sh	Установка ограничений интерфейса оператора.
open.sh	Снятие ограничений интерфейса оператора.
check.sh	Проверка установки ограничений оператора.

В результате выполненных действий функции учетной записи **algont** будут ограничены – запрещен доступ к виртуальным консолям, монтирование CD-дисков и USB-флеш-накопителей. Среда закрыта. Клиент удалённого доступа отсутствует.

В случае возникновения аварийной ситуации или технической необходимости оператор АРМ «АССаД-Видео» может завершить сеанс пользователя ОС, выполнить выключение или перезагрузку компьютера.

При необходимости администратор безопасности выполняет перезагрузку любого компьютера АРМ выполнив вход в ОС с помощью учетной записи **root**.

3 РЕАЛИЗАЦИЯ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

3.1 Организация доступа к программе

Доступ пользователей к информации является авторизованным. Аутентификация пользователя производится по логину и паролю.

3.1.1 Точкой входа пользователя в систему «АССаД-Видео» (Рисунок 1) является модуль пользовательского сервиса (GUI). Модуль пользовательского сервиса непосредственно не проводит аутентификацию, а делегирует эту задачу сервису управления пользователями, паролями и ролями m7-accounts.

3.1.2 Имя пользователя и пароль передаются сервису m7-accounts для определения принципиальной возможности пользователя подключиться к веб-серверу.

3.1.3 Пароль пользователя должен соответствовать параметрам, указанным в Требованиях к сертифицируемым прикладным продуктам ИТ по классам защищённости АСФЗ (Руководящий документ «Системы физической защиты ядерных объектов. Автоматизированные системы физической защиты. Защита информации от несанкционированного доступа. Требования безопасности информации» (приложение №3 к приказу Госкорпорации «Росатом» № 1/669-П 2011 г.):

–срок действия пароля не более 1-го месяца при использовании системы «АССаД-Видео» в АСФЗ 1 класса защищённости;

–срок действия пароля не более 3-х месяцев при использовании системы «АССаД-Видео» в АСФЗ 2 класса защищённости;

–длина пароля не менее 6 алфавитно-цифровых символов;

–формируемый пароль должен включать заглавные и прописные буквы, цифры и специальные знаки (! " # \$ % & ' () * + , - . / : ; < = > ? [\] ^ _ ` { | } ~ , пробел);

–пароль должен быть уникальным, отличающимся не менее, чем 3 символами, среди любых не менее 24 последовательно используемых паролей при использовании системы «АССаД-Видео» в АСФЗ 1 класса защищённости и не менее 12 последовательно используемых паролей при использовании системы «АССаД-Видео» в АСФЗ 2 класса защищённости.

3.1.4 Если авторизационные данные пользователя введены верно, сервис m7-accounts возвращает пару токенов (программных ключей) - токен авторизации и токен обновления. Токены состоят из трех частей: заголовок, полезная нагрузка (логин, роли, срок действия токена) и цифровая подпись. Токены хранятся в БД сервиса m7-accounts. Токен авторизации является ключом доступа к сервисам системы «АССаД-Видео». Токен обновления используется для получения новой пары токенов по истечении срока действия токена авторизации, равного 30 минутам. Токены, срок действия которых истек (просроченные), уничтожаются. В случае неверных данных пользователя токен не выдается и возвращается ошибка — вход в систему не выполняется и пользователю сообщается о причине недопуска и повторно предлагается пройти авторизацию.

3.1.5 После успешной авторизации пользователя в системе модуль пользовательского сервиса обращается к сервису системы, используя выданный пользователю токен авторизации. Служба проверяет корректность токена на основе проверки электронной подписи и срока действия токена. Если токен корректный, осуществляется доступ пользователя к запрашиваемой службе. Процедура проверки токена будет повторяться при каждом обращении к службе. Если токен корректный, но срок его действия истек, он автоматически продлевается модулем пользовательского интерфейса.

3.1.6 При первом запросе пользователя сервис m7-accounts проверяет наличие данного пользователя в БД и сравнивает представленный пароль с паролем пользователя в БД. Также проверяется признак блокирования оператора и срок действия пароля, а также зарегистрирован ли компьютер, с которого идет запрос, в системе.

3.1.7 При дальнейших запросах используется идентификатор сессии для быстрого прохождения аутентификации без выполнения всех проверок. Сессия существует до тех пор, пока пользователь не выйдет из системы, или если пользователь длительное время не выполняет запросов к серверу (по умолчанию — 1 час).

3.1.8 Выход пользователя из системы выполняется нажатием на кнопку «Выход» в браузере. После выхода пользователя из системы сервис аутентификации выполняет уничтожение токена.

3.1.9 Если аутентификация пользователя прошла неудачно, в системе формируется событие об отказе пользователю в доступе с указанием причины.

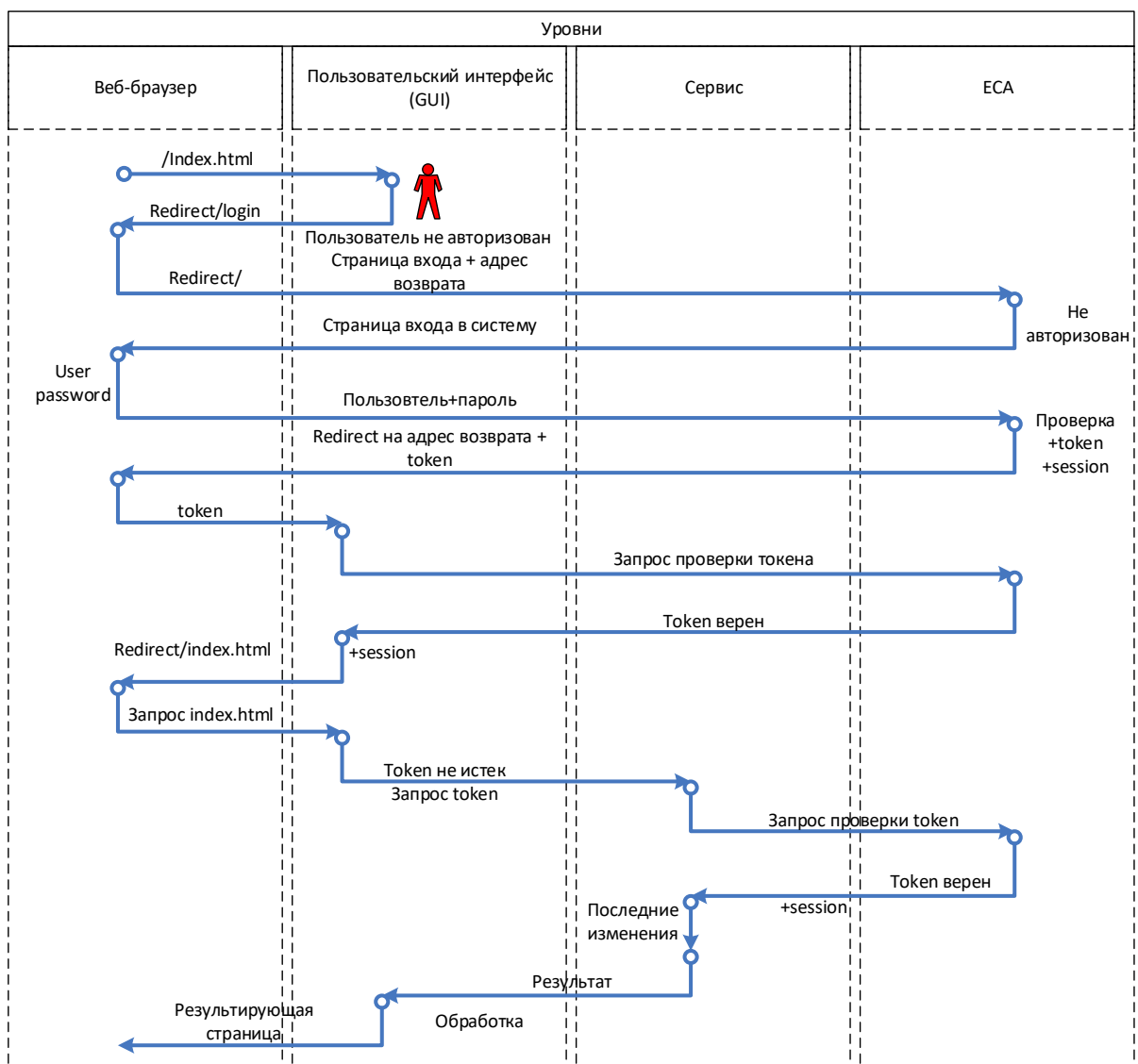


Рисунок 1 — Алгоритм функционирования СЗИ

3.2 Контроль над действиями пользователей

Полномочия пользователя для доступа к отдельным объектам системы определяются ролями, назначенными пользователю.

Все действия пользователя по просмотру и изменению информации протоколируются в журнале событий.

Доступ к средствам сервера осуществляется посредством механизма веб-сервисов.

Разрешение на вызов метода веб-сервиса определяется ролью пользователя. Решение о разрешении доступа к методу определяется до вызова самого метода.

3.2.1 При каждом вызове метода сервиса выполняется проверка роли пользователя. Если пользователь не обладает ролью, необходимой для выполнения метода, запрос завершается с ошибкой.

Пользователи с ролью «Администратор безопасности» получают доступ ко всем методам веб-сервисов системы.

3.2.2 Структура проектируемых таблиц БД обеспечивает целостность данных: ограничение доменов атрибутов, целостность сущностей, ссылочную целостность.

3.2.3 Реализованы ограничения целостности для однозначного соответствия любого изменения информации в таблицах БД с конкретным пользователем системы, с целью исключения возможности изменения информации пользователем СУБД, не являющимся пользователем системы.

3.2.4 Событие «Вход в систему» регистрируется после успешной авторизации пользователя на сервере.

3.2.5 Неудачная попытка входа в пользовательский интерфейс регистрируется с указанием причины отказа в доступе:

- неизвестный пользователь;
- неверный пароль;
- пользователь заблокирован;
- истек срок действия пароля.

3.2.6 Событие «Выход из системы» регистрируется при нажатии кнопки «Выход» в пользовательском интерфейсе или через 60 минут бездействия.

3.3 Контроль доступа к оборудованию

Для контроля доступа к компьютерному оборудованию системы «АССаД-Видео» используется ИБП APC, оснащенный картой сетевого управления (Network Management Card). Например: NMC AP9616, AP9617, AP9618, AP9630, AP9810. ИБП размещается в стойке вместе с компьютерным оборудованием.

Контроль доступа к оборудованию осуществляется посредством Модуля контроля доступа к оборудованию, который устанавливается на любой из компьютеров из состава системы «АССаД-Видео». Модуль позволяет получать уведомления об открытии и закрытии стойки, в которой размещено компьютерное оборудование.

К вводу 1 типа «сухой контакт» карты сетевого управления подключается датчик вскрытия стойки, в которой размещено компьютерное оборудование.

При активизации входа в системе регистрируется событие «Стойка открыта», при возвращении в нормальное состояние — «Стойка закрыта». Сигналы ввода 2 не обрабатываются.

При попытке доступа к стойке в программе выдаются соответствующие уведомления об изменении состояния. Обработка уведомлений Модуля контроля доступа к оборудованию осуществляется аналогично этому процессу для других уведомлений системы.

4 КОНТРОЛЬ ЦЕЛОСТНОСТИ СЗИ

4.1 Общие сведения

СПО «АССаД-Видео» обеспечивает автоматический (ежедневный) и автоматизированный (по команде оператора) контроль целостности СЗИ, входящих в его состав.

Приложение контроля целостности выполняет проверку контрольных сумм на узлах, которые настроены в системе.

На каждом из узлов должен быть установлен сервис **Агент расчета контрольных сумм** (m7-checksum-agent).

При первом запуске проверки необходимо записать эталонные контрольные суммы в БД нажатием на кнопку **Добавить** из списка по умолчанию. В список по умолчанию входят файлы, приведенные в файле gostsumsIST.txt, расположенном на установочном диске ЦРПА.467371.029 или в архиве обновления (порядок предоставления обновлений приведен в Приложении А настоящего документа).

Кроме файлов из списка по умолчанию для сетевого узла можно задать дополнительные файлы, подлежащие контролю. Для добавления файла в поле для ввода необходимо ввести путь к файлу и нажать на кнопку **Добавить**. После этого эталонные контрольные суммы файла будут записаны в БД. В случае, если указанный файл не найден, будет выведено уведомление «не удалось подключение».

Файлы из списка по умолчанию и дополнительные файлы для проверки, добавленные администратором безопасности вручную, составляют список проверяемых файлов для данного сетевого узла.

При проверке СЗИ выполняется расчет контрольных сумм файлов из списка проверяемых файлов и производится сравнение полученных значений с эталонными значениями, хранящимися в БД. По результату сравнения формируются события «Проверка контрольных сумм завершена успешно» (если значения совпадают) или «Проверка контрольных сумм завершена с ошибками» (если значения не совпадают).

4.2 Автоматический и автоматизированный контроль целостности файлов

Автоматическая периодическая проверка контрольных сумм выполняется ежедневно в 01:00.

Ручной запуск проверки контрольных сумм выполняется пользователем с правами администратора безопасности из пользовательского интерфейса приложения **Контроль целостности** с помощью кнопки «Проверить» (для каждого сетевого узла). Результатом ручной проверки является уведомление о ходе проверки контрольных сумм (Рисунок 2).

В случае успешной проверки в поле сетевого узла изменится дата/время проверки. Если проверка контрольных сумм прошла с ошибками, выводится надпись: «Проверка контрольных сумм прошла с ошибками» и выдается соответствующее уведомление. Подробное описание ошибки доступно в **Журнале безопасности**.

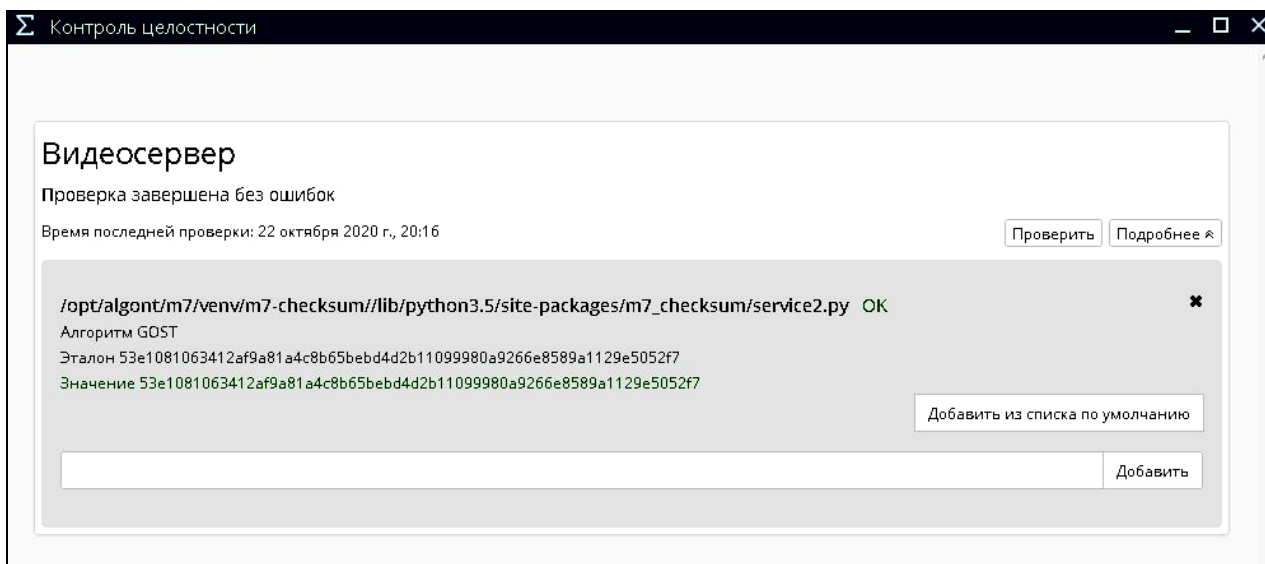


Рисунок 2 — Приложение контроля целостности

4.3 Тестирование СЗИ

СПО «АССаД-Видео» позволяет выполнить проверку работы основных функций СЗИ (авторизация и контроль доступа оператора) в автоматизированном режиме.

Тестирование работы СЗИ на наличие ошибок выполняется на странице **Тестирование** (Рисунок 3) приложения **Учетные записи**.

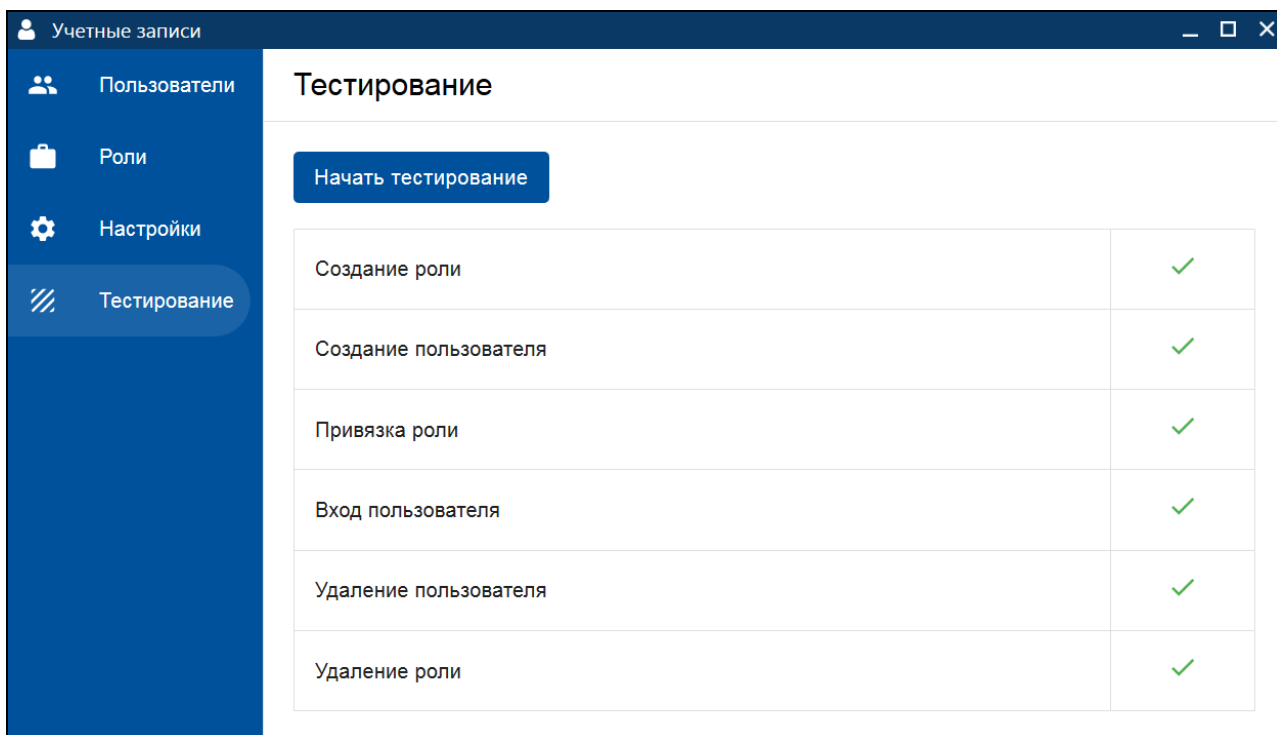


Рисунок 3 — Тестирование

Для начала тестирования необходимо нажать кнопку **Начать тестирование**.

Если во время тестирования возникает исключение, его текст отображается в соответствующем поле.

В процессе тестирования автоматически выполняются следующие операции:

- создание роли;
- создание пользователя;
- привязка роли;
- вход пользователя;
- удаление пользователя;
- удаление роли.

В процессе выполнения операций на экране отображаются выполняемые действия. Процедура тестирования считается успешной, если в ее процессе ошибок не выявлено.

События системы, инициированные во время тестирования приложения, не записываются в журналы событий системы.

5 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ОПЕРАТОРОВ

Доступ к пользовательскому интерфейсу программы выполняется по доменному имени видеосервера, например, <http://shell.algont/>.

В закрытой среде запуск пользовательского интерфейса программы выполняется автоматически при старте системы.

Получить доступ к веб-интерфейсу программы может только зарегистрированный пользователь СПО «АССаД-Видео» (Рисунок 4).

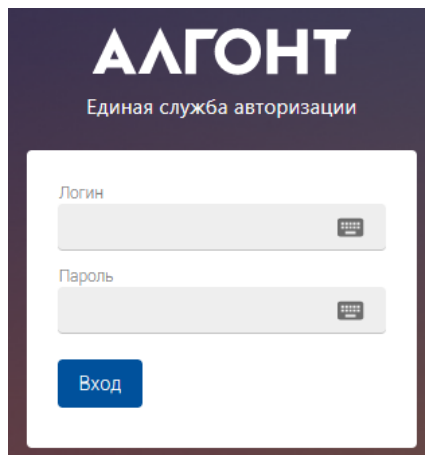


Рисунок 4 – Страница авторизации

Если учетные данные введены верно, будет выполнен переход на страницу по работе с программой, в противном случае будет выведен текст ошибки.

Примечание — Пользователь с учетной записью администратора безопасности, имеет доступ ко всем функциональным возможностям программы.

5.1 Приложение Учетные записи

Приложение **Учетные записи** является приложением платформы «М7», предназначенным для назначения ролей, управления учетными записями пользователей, настройки параметров безопасности и проверки целостности системы.

Доступ к приложению выполняется из **Меню М7** (Рисунок 5).

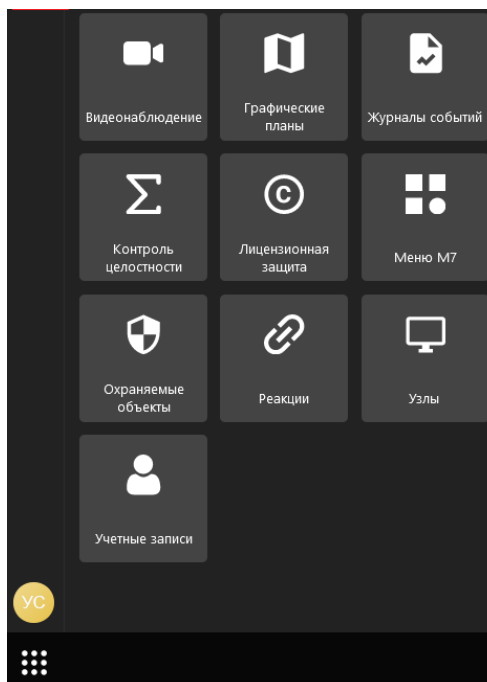


Рисунок 5 - Меню доступа к приложениям

На странице приложения **Учетные записи** по умолчанию открывается вкладка со списком зарегистрированных в программе пользователей (Рисунок 6).

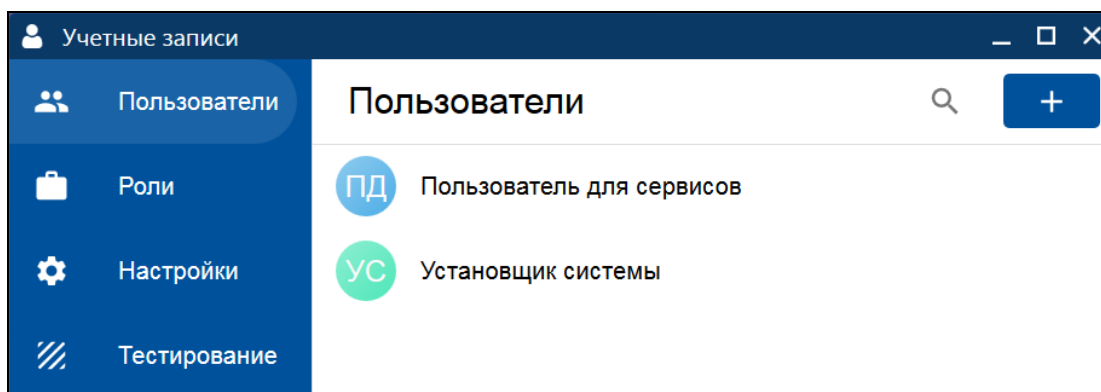


Рисунок 6 — Вкладка **Пользователи** страницы приложения **Учетные записи**

Приложение **Учетные записи** предоставляет следующие возможности:

- **Пользователи** (управление пользователями);
- **Роли** (управление ролями);
- **Настройки** (настройка параметров безопасности пароля);
- **Тестирование** (тестирование работы СЗИ, см. п. 4.3).

Настройку рекомендуется начинать с ролей. Для этого необходимо выбрать вкладку **Роли**.

5.1.1 Управление ролями

На странице **Учетные записи** → **Роли** (Рисунок 7) доступен перечень зарегистрированных в программе ролей.

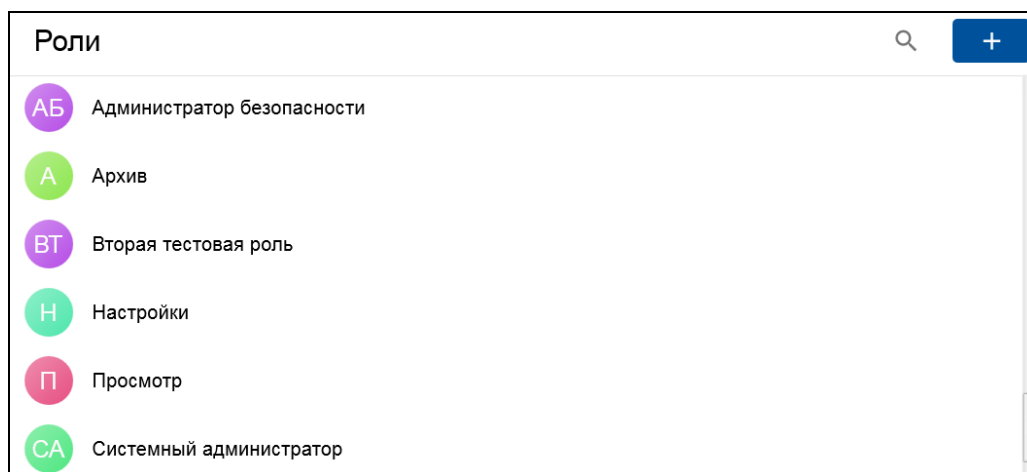


Рисунок 7 – Вкладка **Роли** страницы приложения **Учетные записи**

Для добавления новой роли воспользуйтесь кнопкой «+». В открывшемся окне введите идентификатор роли, название и нажмите кнопку **Сохранить** (Рисунок 8).

ВНИМАНИЕ! Идентификатор роли должен содержать обязательный префикс «ROLE_» и набор символов, назначенных администратором безопасности. К использованию разрешены латинские буквы, цифры и знак подчеркивания «_».

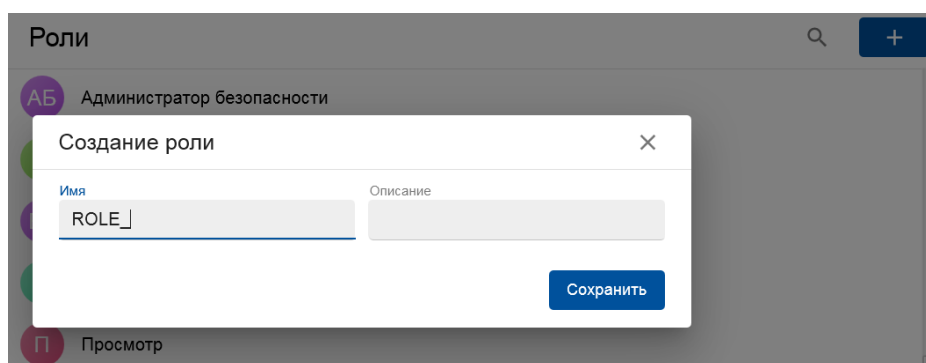


Рисунок 8 – Добавление роли

Для просмотра данных роли или внесения изменений, выберите роль из списка, откроется окно редактирования роли. Для внесения изменений в поле **Имя** нажмите указателем мыши на поле, выполните корректировку и нажмите на кнопку **Сохранить**. Для отмены операции нажмите клавишу Esc или нажмите указателем мыши в свободной области страницы.

Для удаления роли выполните последовательно **⋮** → **Удалить** на странице редактирования роли (Рисунок 9). Для защиты от ошибочных действий оператора системы операция по удалению роли требует подтверждения.

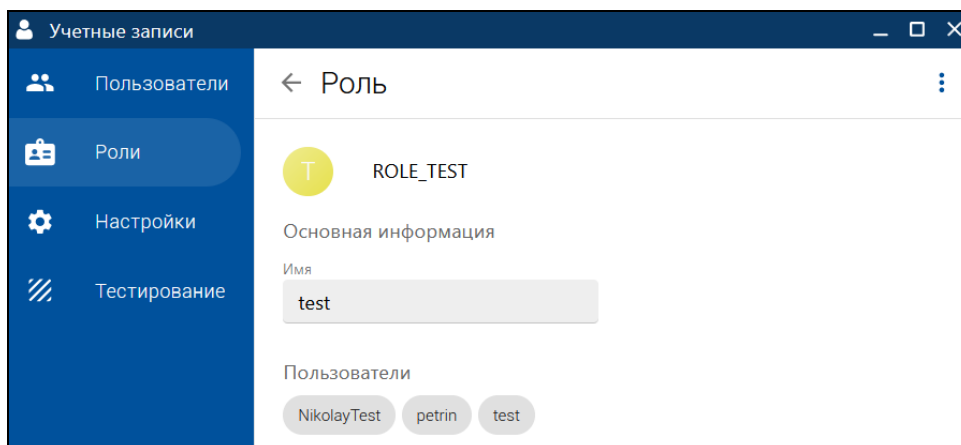


Рисунок 9 – Страница редактирования роли

Следует учесть, что в программе предусмотрены предустановленные (системные) роли (Рисунок 10). В таблице 2 приведено описание предустановленных (системных) ролей.

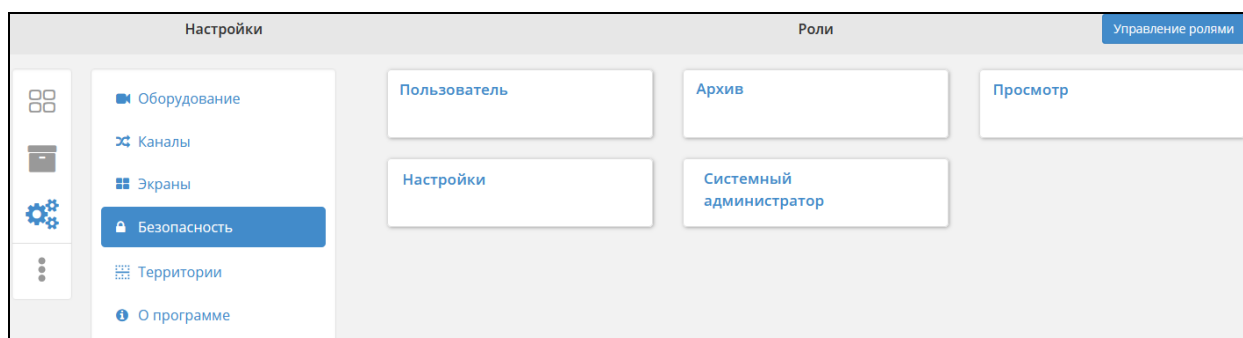


Рисунок 10 — меню **Безопасность** приложения **Видеонаблюдение**

ВНИМАНИЕ! Для обеспечения бесперебойной работы СПО «АССаД-Видео» не рекомендуется вносить изменения в системные роли.

Таблица 2 - Описание системных ролей

Роль	Описание	Доступные пункты меню М7
Администратор безопасности	Полный доступ ко всем данным системы: добавление, изменение, удаление информации об абонентах, настройка (параметры системы, пользователи, серверы и т. д.), просмотр журналов и формирование отчетов о безопасности и системных отчетов.	Узлы Видеонаблюдение (Настройки, Просмотр, Архив) Журнал событий Сценарии Учетные записи Контроль целостности
Системный администратор	Полный доступ, за исключением возможности регистрации в системе новых пользователей и построения отчета о безопасности.	Узлы Видеонаблюдение (Настройки, кроме управления ролями), Просмотр, Архив) Сценарии Изменение профиля (для просмотра, редактирования описания и изменения пароля доступна только своя учетная запись) Журнал событий (кроме журнала безопасности)
Пользователь	Нет разрешений	Описательная роль, присваивается

Роль	Описание	Доступные пункты меню М7
		по умолчанию
Архив	Пользователь получает доступ к функциям просмотра архива	Видеонаблюдение (Архив, в зависимости от прав доступа)
Просмотр	Пользователь получает доступ к работе в системе в режиме мониторинга	Видеонаблюдение (Просмотр, в зависимости от прав доступа)
Настройки	Пользователь получает доступ к настройкам, для администраторов системы	Видеонаблюдение (Настройки, кроме управления ролями)

ВНИМАНИЕ! Для обеспечения бесперебойной работы СПО «АССаД-Видео» не рекомендуется вносить изменения в системные роли.

5.1.2 Настройка параметров безопасности пароля

До начала процесса создания пользователей необходимо настроить параметры безопасности для паролей, соответствующие требованиям к уровням доверия для конкретного АСФЗ. Далее приведены настройки безопасности пароля при использовании системы «АССаД-Видео» в АСФЗ 2 класса защищённости.

В приложении **Учетные записи** открыть пункт меню **Настройки** (Рисунок 11).

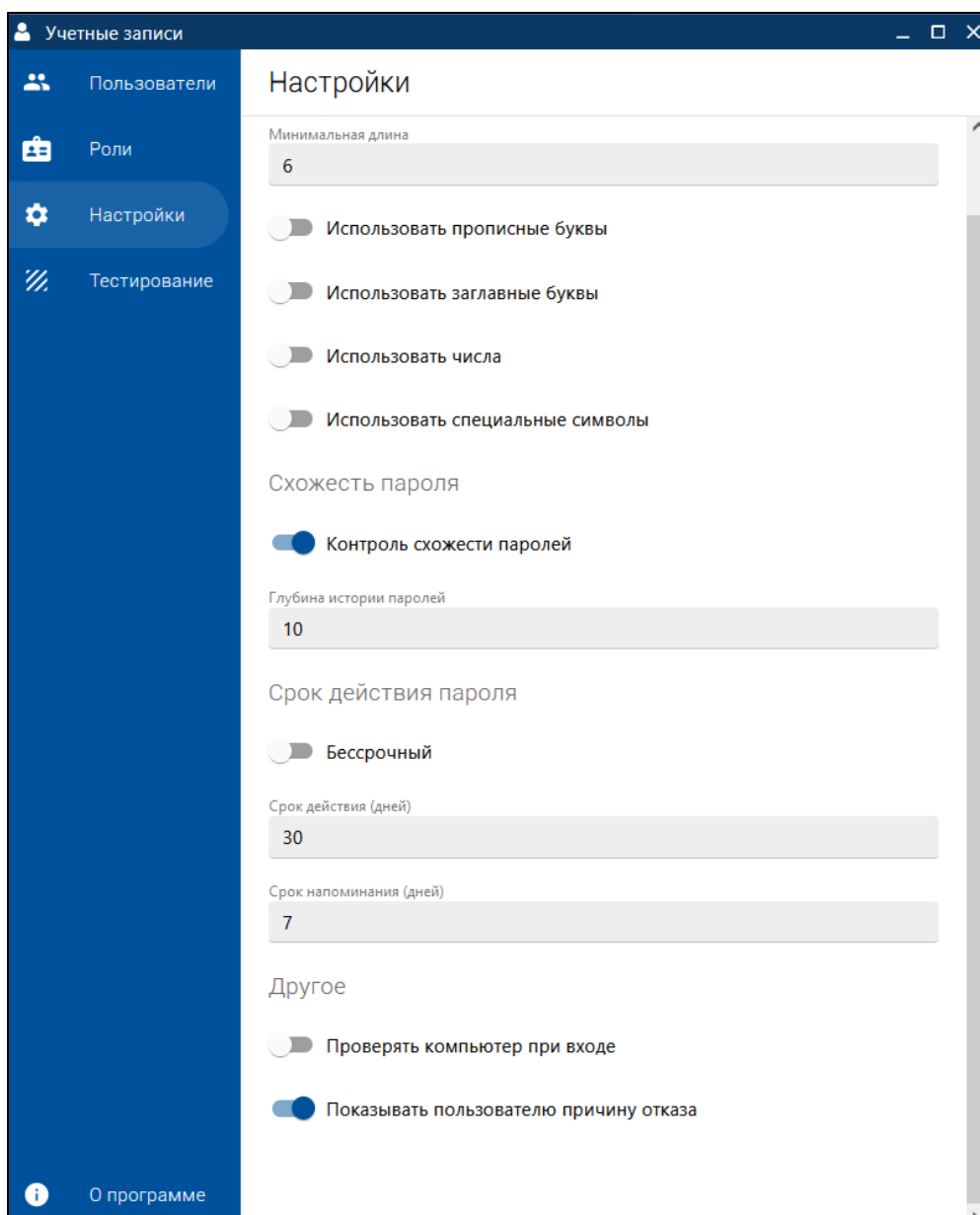


Рисунок 11 — Страница Настройки параметров безопасности

Описание параметров приведено в таблице 3.

Таблица 3 – Описание параметров безопасности

Параметр	Описание	Ограничения
Минимальная длина пароля	Минимальное количество символов в пароле.	см. п. 3.1.3
Глубина истории паролей	Количество паролей, с которыми сравнивается новый пароль на предмет точного совпадения. В случае совпадения с одним из таких паролей новый пароль считается некорректным	см. п. 3.1.3
Срок действия паролей, дней	Срок, в течение которого любой пароль системы активен. По истечению срока действия пароля, он считается устаревшим. Вход в систему с таким паролем невозможен	см. п. 3.1.3
Контроль схожести	Пароль должен быть уникальным,	см. п. 3.1.3

Параметр	Описание	Ограничения
	отличающимися не менее, чем 3 символами	
Хотя бы одна цифра в пароле	Среди набора символов пароля должна присутствовать как минимум одна цифра	см. п. 3.1.3
Прописные и строчные буквы в пароле	Среди набора символов пароля должна присутствовать как минимум одна прописная и одна строчная буква	см. п. 3.2.2
Хотя бы один спец. символ в пароле	Среди набора символов пароля должен присутствовать как минимум один спецсимвол из набора: «! @ # \$ % ^ & * () - _ + = ; : , . / ? \ ` ~ [] { } »	см. п. 3.2.2

5.1.3 Управление пользователями

Для добавления нового пользователя воспользуйтесь кнопкой «+» (Рисунок 12).

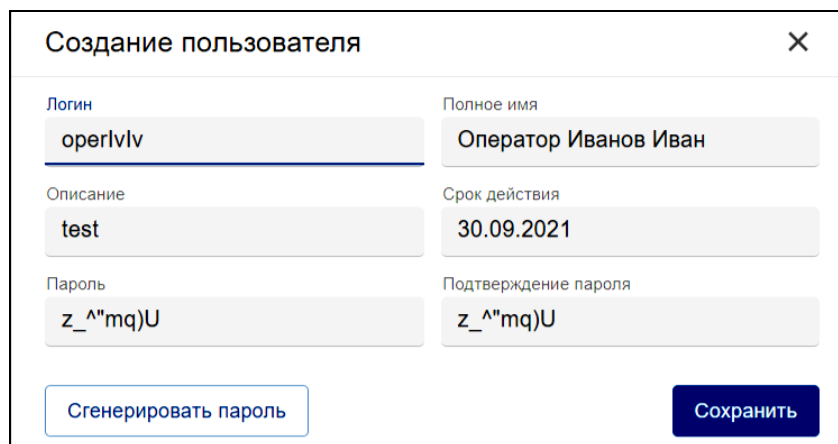


Рисунок 12 — Окно создания учетной записи пользователя

В окне **Создание пользователя** введите **Логин**, **Полное имя** нового пользователя (будет отображаться в программе), **Описание**, **Пароль** и его **Подтверждение**, после сохранения выберите роль (роли) из списка. На странице создания пользователя автоматически проставляется дата окончания срока действия заданного пароля в соответствии с настройками, заданными в **Настройках политики безопасности**.

Для редактирования информации о пользователе выберите нужную запись и внесите необходимые корректировки (Рисунок 13). Переключатель **Заблокирован** позволяет временно заблокировать пользователя, элемент **Срок действия** служит для отображения срока действия пароля пользователя в соответствии с установленными в программе ограничениями. При необходимости срок действия пароля может быть изменен.

В нижней части окна отображается список ролей, назначенных выбранному пользователю.

5.1.4 Назначение ролей

Для того чтобы назначить пользователю уже настроенную роль, необходимо открыть карточку учетной записи и с помощью кнопки **+** подобрать роль из выпадающего списка, для удаления роли – на кнопку **×**.

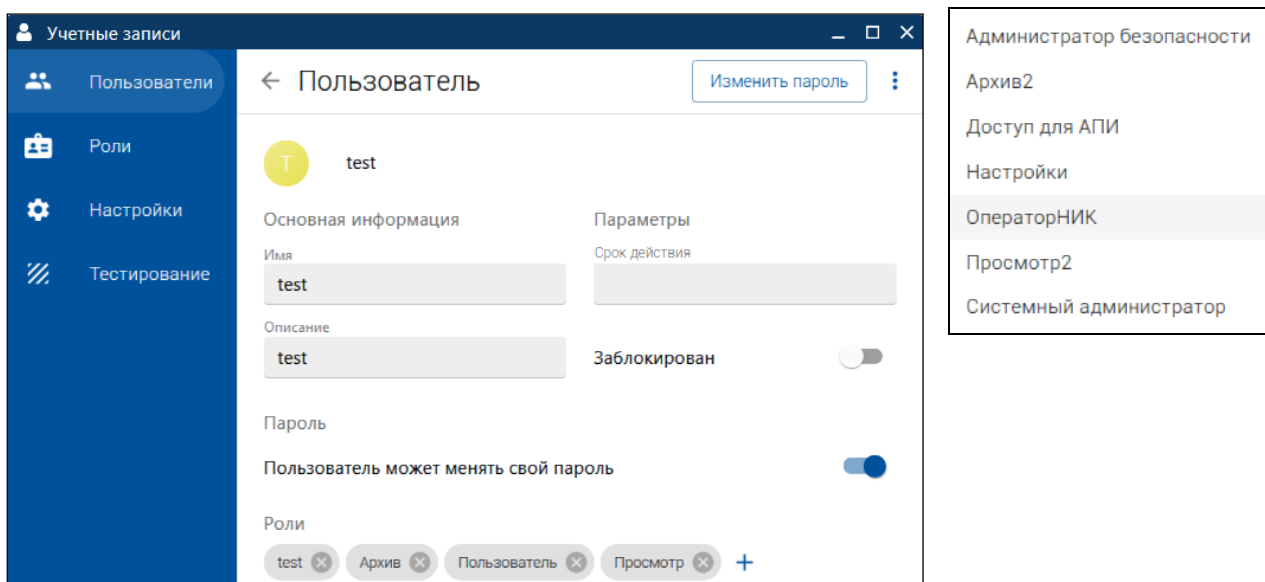


Рисунок 13— Окно редактирования учетной записи

Например, при добавлении в систему пользователя, который является оператором наблюдения и не должен иметь доступ к просмотру архива, должна быть назначена роль **Просмотр**, роли **Архив**, а роль **Настройки** не должны быть назначены.

Для каждой роли необходимо задать отображение доступных приложений в меню М7 в соответствии с указаниями раздела 8 настоящего Руководства.

Для удаления учетной записи выполните последовательно **⋮** → **Удалить** в режиме редактирования параметров пользователя. Для защиты от ошибочных действий оператора системы операция по удалению пользователя требует подтверждения.

ВНИМАНИЕ! В СПО «АССаД-Видео» запрещается выполнять любые манипуляции с сервисным пользователем «М7».

6 НАСТРОЙКА ДОСТУПА К ЭКРАНАМ И КАНАЛАМ

Настройка прав доступа пользователей к экранам и каналам выполняются во вкладке **Безопасность** настроек приложения **Видеонаблюдение** (Рисунок 14). Права доступа назначаются ролям, выданным пользователям. Для перехода к перечню ролей в меню М7 необходимо нажать на кнопку **Управление ролями**.

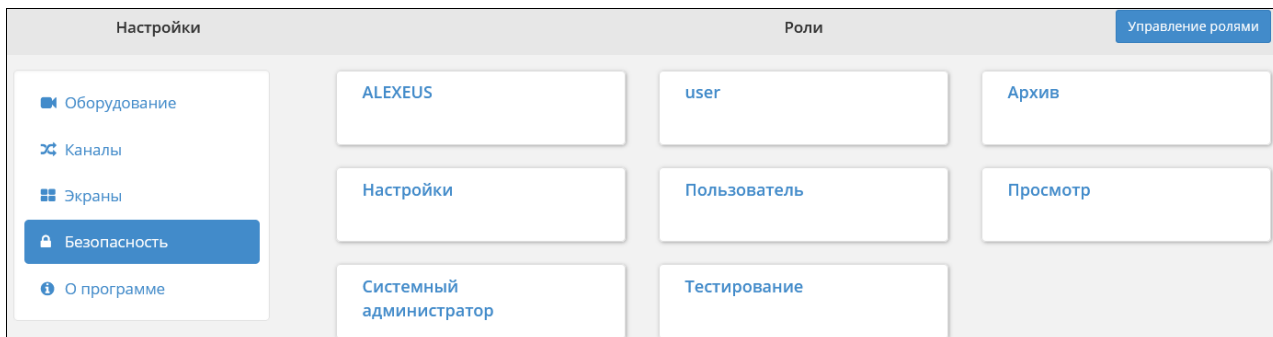


Рисунок 14 – Страница Безопасность

При выборе роли открывается страница редактирования прав доступа (Рисунок 15).

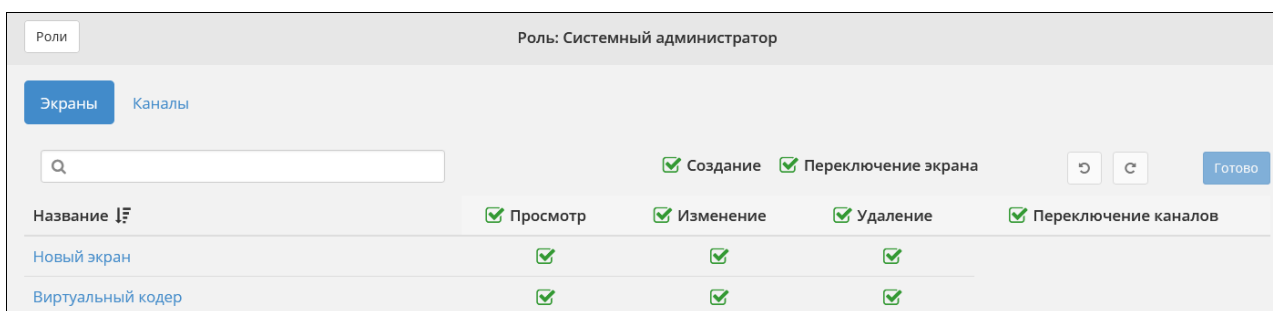


Рисунок 15 — Окно редактирования прав доступа для роли

Отдельно настраиваются права доступа для **Экранов** (экран представляет собой совокупность ячеек отображения потоков живого видео, графпланов и других элементов визуализации с целью обеспечения функций контроля обстановки на объекте) и **Каналов** (под каналом в данном случае подразумевается объект программы, с которым сопоставлены потоки живого видео от видеоканалов и потоки аналитики). Во вкладке **Экраны** слева находится список экранов, для которого предусмотрена возможность поиска и сортировки.

Для каждого экрана можно настроить права доступа: **Создание, Просмотр, Изменение, Удаление и Переключение каналов**.

Параметр	Функции системы	Предоставляемые права
Создание	Настройка	Позволяет пользователю создавать экран.
Просмотр	Просмотр, Архив	Позволяет пользователю просматривать данные экрана.
Изменение	Настройка	Позволяет пользователю изменять свойства экрана.
Удаление	Настройка	Позволяет пользователю удалять экран.
Переключение экрана	Настройка	Позволяет пользователю изменять отображаемый экран на мониторе АРМ.
Переключение каналов	Настройка	Позволяет пользователю изменять отображаемый канал в ячейке.

Активировав параметр в верхней строке таблицы назначения прав доступа, можно разрешить или запретить выполнение выбранного действия для всего списка экранов.

Управляя параметрами активации напротив конкретного экрана, можно, соответственно, разрешить или запретить выполнение с ним выбранного действия.

Аналогично настраиваются разрешения для выполнения действий с каналами (Рисунок 16).

Название	Просмотр	Изменение	Удаление	Запись	Снимок	Архив	Скачать	Взятие под охрану	PTZ	Приоритет PTZ
MediaCanal_10.1.5.137	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2
MediaCanal_10.1.5.18	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0

Рисунок 16 – Назначение разрешений для действий с каналами

Параметр	Функции системы	Предоставляемые права
Создание	Настройка	Позволяет пользователю создавать канал.
Просмотр	Просмотр, Архив	Позволяет пользователю просматривать данные канала.
Изменение	Настройка	Позволяет пользователю изменять свойства канала.
Удаление	Настройка	Позволяет пользователю удалять канал.
Запись	Просмотр	Позволяет пользователю осуществлять запись по каналу.
Снимок	Просмотр	Позволяет пользователю создавать снимок по каналу.
Архив	Архив	Позволяет пользователю просматривать архивные видеозаписи по каналу.
Скачать	Архив	Позволяет пользователю выполнять скачивание видеозаписей по каналу.
Взятие под охрану	Реакции на события	Позволяет пользователю поставить канал под охрану или снять с охраны.
PTZ	Просмотр	Позволяет пользователю осуществлять настройки PTZ оборудования, прикрепленного к каналу.
Приоритет PTZ	Просмотр	Всего приоритетов PTZ в системе 6 (от 0 до 5). PTZ = 0 устанавливается по умолчанию. PTZ = 5 является наивысшим для функции управления PTZ для данного канала. Особенности управления PTZ-видеокамерами пользователями с различными приоритетами изложены в п. 3.3.6 Руководства оператора ЦРПА.2.00124.01.00 34

7 РЕГИСТРАЦИЯ СОБЫТИЙ

Все действия по просмотру и изменению информации регистрируются в БД СПО «АССаД-Видео».

Работа с уведомлениями состоит в обработке тревожных событий в **Панели уведомлений** (Рисунок 17).

В **Панели уведомлений** элементы группируются по приложению-инициатору (например, **Видеонаблюдение** или **Учетные записи**).

Подтвердить уведомление можно, нажав на **✕** в строке уведомления. Очистить список уведомлений можно нажатием на кнопку **✕** в строке приложения-инициатора. Уведомления описаны в таблице 4.

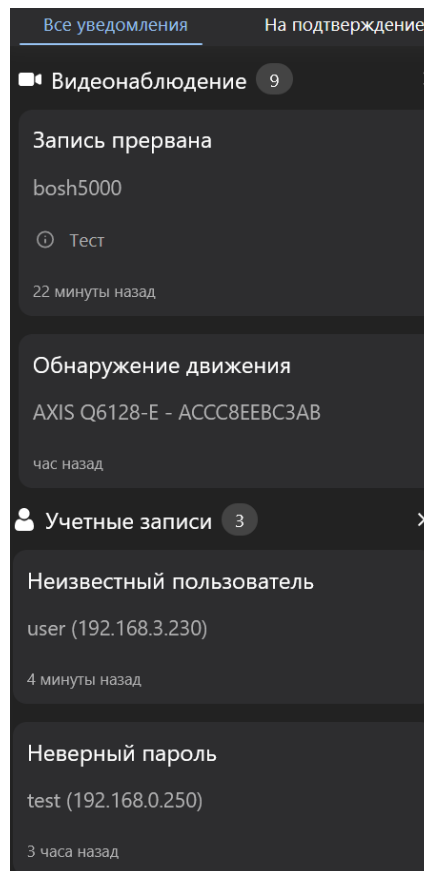


Рисунок 17 — Уведомления

Для того, чтобы взять тревожное событие в обработку, достаточно нажать на него указателем мыши.

При генерации события уведомление дублируется в форме всплывающего сообщения, которое призвано привлечь внимание пользователя и отображается на экране монитора в течении 5 с.

Для всплывающих сообщений доступно закрытие нажатием на кнопку «X».

Таблица 4 — Уведомления приложений

Уведомление	Инициатор	Описание	Действия администратора безопасности
Отказано в доступе	Учетные записи	Формируется в случае неудачной попытки входа пользователя в систему. Данным уведомлением оповещаются все	Необходимо связаться с оператором, пытавшимся зарегистрироваться в системе

Уведомление	Инициатор	Описание	Действия администратора безопасности
		операторы системы.	
Нет связи с узлом	Контроль целостности	Уведомление формируется, если отсутствует связь с устройством при попытке проверки контрольных сумм	Рекомендуется проверить физическое подключение оборудования узла
Контрольные суммы не совпадают с эталоном	Контроль целостности	Уведомление формируется в случае неудачной проверки контрольных сумм, если полученные в результате проверки контрольные суммы отличны от эталона	Необходимо сверить КС с Формуляром и при несовпадении исключить возможность несанкционированного доступа к вызвавшему ошибку сетевому узлу. Проверить настройку закрытия среды на этом сетевом узле в соответствии с данным руководством, переустановить СПО «АССаД-Видео» в соответствии с Руководством системного программиста.
Контрольные суммы инициализированы - формируется при первой проверке контрольных сумм	Контроль целостности	Инициализация контрольных сумм осуществлена	Действия не предусмотрены
Внутренняя ошибка при проверке контрольных сумм	Контроль целостности	Уведомление формируется в случае неудачной проверки контрольных сумм, если во время проверки произошла внутренняя ошибка системы	Рекомендуется произвести повторную проверку. В случае повторения ошибки перезагрузить оборудование узла
Стойка открыта	Приложение уведомления	Уведомление формируется в случае, если стойка с оборудованием «АССаД-Видео» была открыта	Проверить реальное физическое состояние стойки. Проверить состояние датчика
Стойка закрыта		Уведомление формируется в случае, если стойка с оборудованием «АССаД-Видео» была закрыта	

8 УПРАВЛЕНИЕ ДОСТУПНОСТЬЮ ПРИЛОЖЕНИЙ В МЕНЮ М7

Управление доступностью приложений в **Меню М7** осуществляется в **Меню приложений** (Рисунок 18).

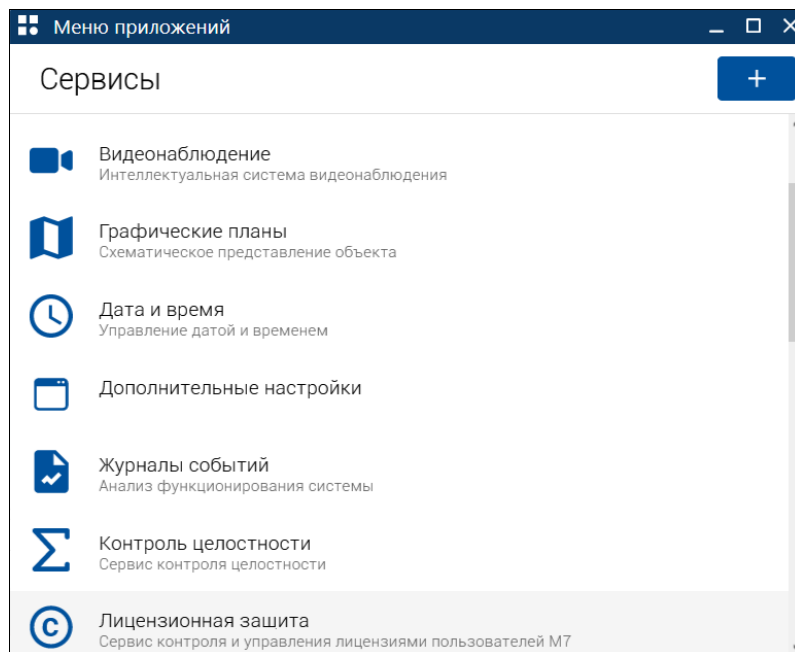


Рисунок 18 — Окно приложения Меню М7

Для перехода к редактированию элемента нажмите на наименование приложения и внесите необходимые корректировки на странице редактирования параметров. В нижней части страницы отображается список ролей, для которых назначено разрешение на отображение приложения в **Меню приложений** (Рисунок 19), администратору безопасности по умолчанию доступны все приложения. После завершения редактирования нажмите кнопку **Сохранить** для применения внесенных изменений.

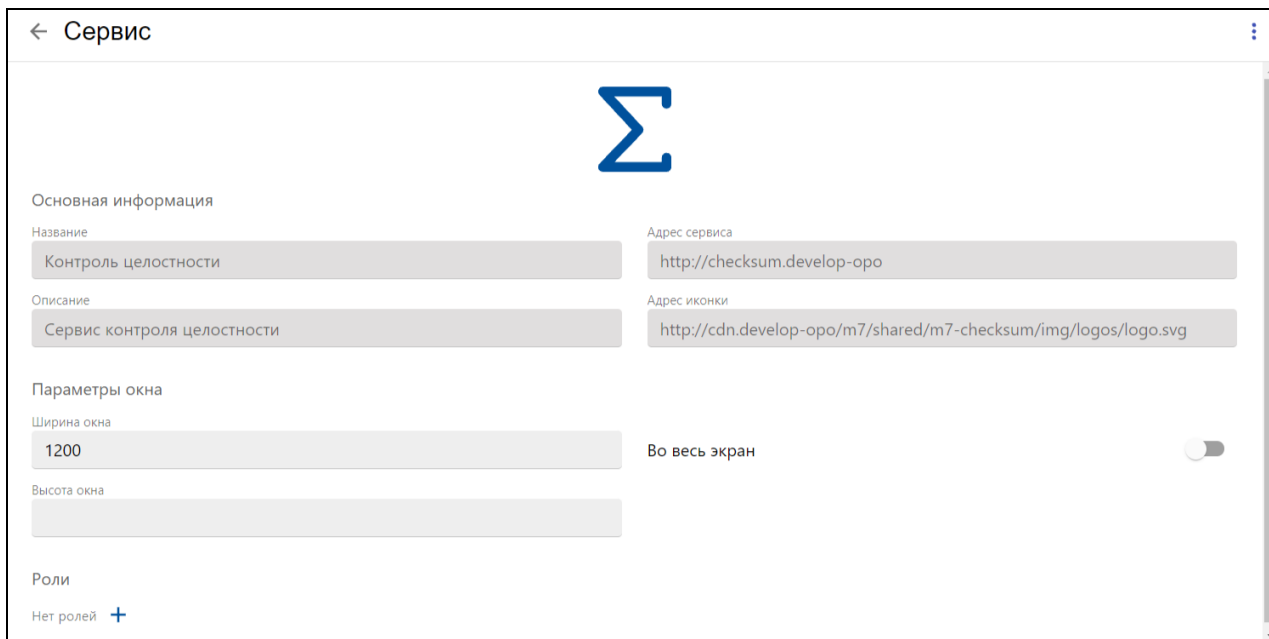


Рисунок 19 — Страница редактирования параметров приложения

Для добавления приложения нажмите на кнопку **Добавить**. В окне добавления приложения (Рисунок 20) заполните предложенные поля в соответствии с рекомендациями:

Наименование параметра	Описание	Пример заполнения
Основная информация		
Название	Текстовый идентификатор приложения в системе	Учетные записи
Адрес приложения	Адрес для доступа к приложению	http://accounts.algont:80 , где (где algont — доменное имя видеосервера, 80 — номер порта)
Адрес иконки	Путь к файлу с иконкой	http://accounts.algont:80/m7-icon.png
Описание	Дополнительная информация о приложении в произвольной форме	—
Параметры окна		
Ширина, Высота, Во весь экран	Для отображения страницы в оболочке Shell можно указать размер по умолчанию, задав Ширину и Высоту окна . Для отображения окна во весь экран необходимо активировать переключатель Во весь экран .	—
Роли		
Роли	Роли, которым назначено разрешение на отображение приложения.	—

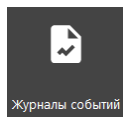
Рисунок 20 — Окно добавления приложения

Завершите добавление нажатием на кнопку **Сохранить**, выполните назначение ролей. После этого новое приложение появится в перечне приложений системы и **Меню М7**.

Примечание – подробное описание основных приложений программы приведено в Руководстве системного программиста ЦРПА.2.00124.01.00 32.

9 ЖУРНАЛЫ СОБЫТИЙ

Все события, произошедшие в системе (тревожные события, срабатывание датчиков движения и т. д.), записываются и хранятся в системе. Доступ к записям событий осуществляется из модуля **Журналы событий**. Доступ к модулю осуществляется из **Меню М7**, нажатием на соответствующую иконку.



Приложение предоставляет доступ к нескольким видам журналов:

Наименование	Описание
Журнал безопасности	Содержит события, отражающие действия пользователей системы (например, подключение пользователя). Позволяет контролировать действия оператора: вход в систему, выход из системы, просмотр, добавление, изменение или удаление данных в конфигурации системы.
Системный журнал	Содержит сведения о событиях, отражающих изменение состояния устройств или каналов связи (например, пропадание связи).
Журнал событий	Представляет перечень событий, связанных с аналитикой (например, появление (прекращение) движения) и событий управления записью – включение, выключение).

Основное описание работы с модулем **Журналы событий** приведено в разделе 13 Руководства системного программиста ЦРПА.2.00124.01.00 32. В настоящем руководстве приведем описание событий **Журнала безопасности, доступного только администратору безопасности**.

Таблица 7 — События журнала безопасности

Событие	Инициатор	Описание
Просмотр объекта	Одно из приложений системы в зависимости от типа объекта	Запрос на предоставление информации об объекте оператором
Добавление объекта		Создан новый элемент системы (например, профиль абонента, медиаканал, устройство).
Удаление объекта		Удален элемент системы (например, медиаканал, устройство).
Изменение объекта		Внесены изменения в параметры объекта (например, к медиаканалу подключено дополнительное оборудование, изменено описание экрана и т. п.).
Формирование отчета		По запросу оператора сформирован отчет
Отключение записи в журнал		Запись в журнал отключена и не ведется
Включение записи в журнал		Запись в журнал включена
Стойка открыта	Приложение уведомления	Стойка с оборудованием системы была открыта
Стойка закрыта		Стойка с оборудованием системы была закрыта
Подключение пользователя	Учетные записи пользователей	Пользователь подключился к серверу «АССаД-Видео» с помощью веб-интерфейса. Регистрация пользователя может быть выполнена с помощью имени пользователя и

Событие	Инициатор	Описание
		пароля.
Отключение пользователя		Оператор вышел из веб-интерфейса. Событие формируется только в том случае, если пользователь нажал кнопку Выйти для выхода.
Неизвестный пользователь		Попытка входа в систему под учетной записью пользователя, не зарегистрированного в системе
Доступ запрещен		Отказ во входе в систему. В деталях события указывается причина отказа в доступе
Добавление пользователя		Добавлен новый пользователь
Изменение пользователя		Изменены параметры существующего пользователя
Удаление пользователя		Пользователь удален
Просмотр пользователя		Просмотр информации о пользователе оператором
Добавление роли		Добавлена новая роль
Изменение роли		Внесены изменения в параметры существующей роли
Удаление роли		Роль удалена
Просмотр роли		Просмотр информации о роли пользователем
Назначение роли		Пользователю назначена роль
Изъятие роли		Изъятие назначенной роли у пользователя
Проверка контрольных сумм завершена успешно	Приложение контроль целостности	В ходе проверки контрольных сумм ошибок не возникло
Проверка контрольных сумм завершена с ошибками		В ходе проверки контрольных сумм возникла ошибка. В деталях события указывается причина ошибки (например, "Нет связи с узлом", "Контрольные суммы не совпадают с эталоном" и проч.)
Постановка под охрану	Приложение охраняемые объекты	Охраняемый объект поставлен под охрану
Снятие с охраны		Охраняемый объект снят с охраны
Просмотр записи	Пользовательский интерфейс	Выполнен просмотр архивной видеозаписи
Скачивание записи	Пользовательский интерфейс	Выполнено скачивание файла видеозаписи

Примечание — Полная информация по событию доступна в форме всплывающего дополнительного окна, для вызова которого необходимо нажать указателем мыши по наименованию события.

10 СООБЩЕНИЯ АДМИНИСТРАТОРУ БЕЗОПАСНОСТИ

Перечень сообщений приведен в таблице 7 настоящего документа.

ПРИЛОЖЕНИЕ А

(обязательное)

ПОРЯДОК УСТРАНЕНИЯ НЕДОСТАТКОВ И УЯЗВИМОСТЕЙ И ДОВЕДЕНИЯ ОБНОВЛЕНИЙ ДО ПОТРЕБИТЕЛЕЙ

Выпуск обновлений СПО «АССаД-Видео» выполняется в рамках проведения процедур по устранению уязвимостей и обеспечивает поддержание СПО в сертифицированном состоянии.

Указанные в настоящем приложении процедуры выполняются в соответствии с «Положением о системе сертификации средств защиты информации ФСТЭК России» (далее – «Положение о сертификации»).

При выявлении уязвимостей СПО «АССаД-Видео» выполняются следующие мероприятия:

- изготовитель разрабатывает меры, обеспечивающие устранение этой уязвимости (например, разработка обновления), или принимает правовые, организационные, технические меры, снижающие возможность эксплуатации уязвимости нарушителем (далее - меры по устранению уязвимости);

- изготовитель публикует информацию о мерах по устранению уязвимости СПО «АССаД-Видео» на официальном сайте <https://algont.ru/bulletin>;

- оповещение потребителей о мерах по устранению уязвимости СПО «АССаД-Видео» средствами рассылки электронных писем, если они известны и зафиксированы в лицензионном договоре или договоре на техническую поддержку ПО между АО «АЛГОНТ» и потребителем;

- конечными потребителями принимаются меры по устранению уязвимостей СПО «АССаД-Видео». Если в процессе соблюдения мер выполнялось обновление СПО, потребитель вносит соответствующие отметки в раздел 12 формуляра.

Доведение информации о мерах осуществляется до каждого потребителя способом, обеспечивающим подлинность и целостность доводимой информации. При доведении информации по сетям связи ее подлинность и целостность обеспечиваются за счет применения электронной подписи (далее – ЭП). При доведении до потребителей обновлений СПО также обеспечивается их подлинность и целостность за счет применения ЭП.

Если потребитель не может реализовать меры по устранению уязвимостей, он прекращает его применение.

Если уязвимость не устраняется путем ограничений по применению, изготовитель незамедлительно и гарантированно, с подтверждением, сообщает об этом всем потребителям и во ФСТЭК России. Потребители прекращают применение СПО «АССаД-Видео».

