УТВЕРЖДЕН
ЦРПА.2.00067.01.00 92-ЛУ

СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ БИОИДЕНТИФИКАЦИИ «АССаД-ID»

Руководство администратора безопасности

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

ЦРПА.2.00067.01.00 92

Листов 27

2024

Изм. 8

Литера

АННОТАЦИЯ

Настоящее руководство администратора безопасности информации содержит сведения по настройке и сопровождению встроенных средств защиты информации от несанкционированного доступа специального программного обеспечения автоматизированной системы биоидентификации «АССаД-ID» (далее по тексту — СПО «АССаД-ID»).

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

Администраторы безопасности информации ответственны за защиту информации от несанкционированного доступа в системе «АССаД-ID». Администраторы безопасности осуществляют управление разграничением доступа операторов и системных администраторов системы «АССаД-ID» 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-ID» описана в руководстве системного программиста ЦРПА.2.00067.01.00 32 и в руководстве оператора ЦРПА.2.00067.01.00 34.

В настоящем документе приняты следующие сокращения:

АРМ — автоматизированное рабочее место;
АПИ — аппаратно-программный интерфейс;
АСФЗ — автоматизированные средства физической защиты;
БД — база данных;
НСД — несанкционированный доступ;
МРД — мандатное разграничение доступа;
ПКМ — программный комплекс мониторинга;
ОС — операционная система;
СЗИ — средства защиты информации;
СКУД — система контроля и управления доступом;
СПО — специальное программное обеспечение;
СУБД — система управления базами данных;
ФСТЭК — Федеральная служба по техническому и экспортному контролю;
AJP — Apache JServ Protocol;
SNMP — Simple Network Management Protocol;
SMTP — Simple Mail Transfer Protocol;
VPN — Virtual Private Network.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ О СРЕДСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

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

– средства аутентификации операторов в СПО «АССаД-ID»;

– средства управления доступом операторов к ресурсам «АССаД-ID», реализованные с помощью ролей;

– средства регистрации событий, произошедших при работе СПО «АССаД-ID»;

– средства обеспечения контроля целостности.

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, настройка и приемка СЗИ НСД осуществляется в следующем порядке:

а) установить ОС «Astra Linux Special Edition» (не ниже очередного обновления версии 1.7) на серверах, станциях распознавания и АРМ согласно руководству системного программиста ЦРПА.2.00067.01.00 32 и документации ОС;

б) установить пароль суперпользователя root на серверах, станциях распознавания и АРМ согласно руководству системного программиста ЦРПА.2.00067.01.00 32;

в) выполнить настройку параметров сети на серверах, станциях распознавания и АРМ согласно руководству системного программиста ЦРПА.2.00067.01.00 32;

г) установить СПО «АССаД-ID» на серверах и станциях распознавания согласно руководству системного программиста ЦРПА.2.00067.01.00 32;

д) установить библиотеку распознавания 3DiVi на станциях распознавания согласно руководству системного программиста ЦРПА.2.00067.01.00 32;

е) установить библиотеку распознавания VisionLabs на станциях распознавания согласно руководству системного программиста ЦРПА.2.00067.01.00 32;

ж) установить антивирусную программу согласно руководству системного программиста ЦРПА.2.00067.01.00 32 и документации антивирусной программы;

з) выполнить настройку ha-кластера на серверах согласно руководству системного программиста ЦРПА.2.00067.01.00 32;

и) выполнить настройку ограничения интерфейса пользователям на АРМ;

к) зарегистрировать сервера, станции распознавания и консоли распознавания в СПО «АССаД-ID»;

л) зарегистрировать пользователей в СПО «АССаД-ID»;

м) убедиться в успешном входе всех зарегистрированных пользователей в систему с АРМ и доступность пунктов меню в соответствии с выбранной ролью;

н) убедиться в успешном подключении к каждому из серверов и успешном проведении тестирования СЗИ на каждом из серверов;

п) последовательно открыть и закрыть двери стоек с оборудованием, убедиться в регистрации сообщений «Стойка открыта» и «Стойка закрыта» в отчете о безопасности;

р) убедиться в регистрации сообщений «Проверка контрольных сумм прошла успешно» в отчете о безопасности при старте серверов и станций распознавания;

с) последовательно выполнить автоматизированный контроль контрольных сумм на каждом сервере и станции распознавания с помощью кнопки «Проверить контрольные суммы», убедиться в отсутствии ошибок.

2 ОГРАНИЧЕНИЕ СРЕДЫ ФУНКЦИОНИРОВАНИЯ

2.1 Общие сведения

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

Для ограничения среды функционирования на АРМ необходимо создать пользователя операционной системы специального назначения «Astra Linux Special Edition» (не ниже очередного обновления версии 1.7) и выполнить настройку киоска для данного пользователя.

Для ограничения среды функционирования на серверах и рабочих станциях необходимо отключить нежелательные протоколы и службы.

Допускается операторам при входе в ОС на АРМ использовать одну учетную запись пользователя ОС (например, algont) или разные учетные записи пользователей ОС.

2.2 Настройка киоска

Для учетной записи пользователя ОС, которую используют операторы для входа в ОС на АРМ, должна быть выполнена настройка киоска, не позволяющая оператору выполнять какие-либо программы и команды ОС, кроме запуска веб-браузера Firefox.

Настройка производится после установки ОС на АРМ согласно руководству системного программиста ЦРПА.2.00067.01.00 32 следующим образом:

1) войти в ОС под учетной записью algont, созданной при установке ОС;

2) выполнить настройку мандатных атрибутов для пользователя root с помощью утилиты управления политикой безопасности fly-admin-smc, для этого:

– перейти в **Панель управления → Безопасность → Политика безопасности;**

– в открывшемся окне в левой панели выбрать **Мандатный контроль целостности** и убедиться, что **Подсистема Мандатного Контроля Целостности** включена;

– в открывшемся окне в левой панели выбрать **Пользователи**, в фильтре на панели инструментов выбрать **Все;**

– выбрать профиль **root**;

– перейти на вкладку **МРД**;

– выбрать целостность «63: Высокий» (рисунок 1);

– нажать кнопку **Применить изменения** на панели инструментов;

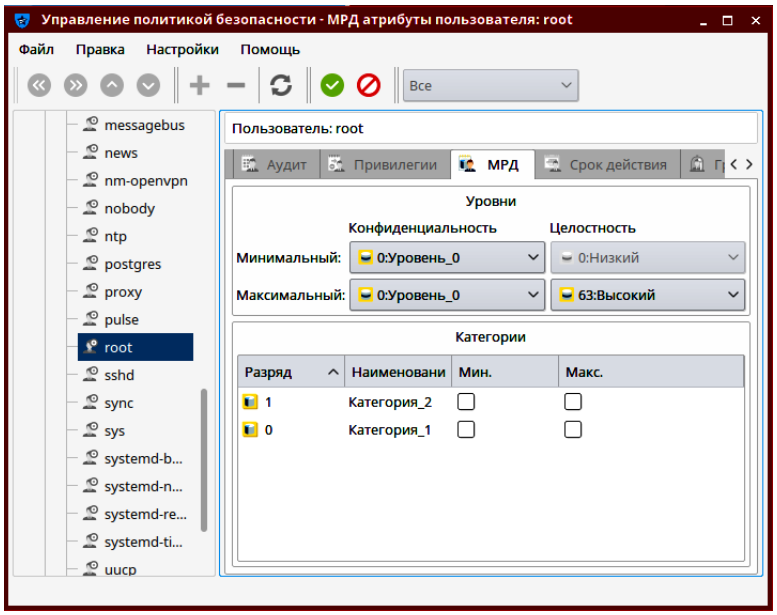

Рисунок 1 — Настройка мандатных атрибутов пользователя root

3) войти в ОС под учетной записью пользователя root;

4) удалить профиль пользователя algont, созданного при установке ОС, следующим образом:

– перейти в **Панель управления → Безопасность → Политика безопасности**;

– в открывшемся окне в левой панели выбрать **Пользователи → algont**;

– нажать кнопку **Удалить элемент** на панели инструментов;

– нажать кнопку **Применить изменения** на панели инструментов.

5) создать профиль пользователя algont с параметрами по умолчанию следующим образом:

– перейти в **Панель управления → Безопасность → Политика безопасности**;

– в открывшемся окне в левой панели выбрать **Пользователи**;

– нажать кнопку **Создать новый элемент** на панели инструментов.

– в поле **Имя** ввести algont;

– нажать кнопку **Применить изменения** на панели инструментов и задать пользователю пароль;

6) распаковать архив install-arm/firefox-arm.tar.gz, содержащий скрипт firefox.sh (реализует ограничения действий пользователей при работе с веб-браузером Firefox) в каталог /home/algont/.

Примечание – В скрипте firefox.sh необходимо предварительно проверить актуальность адреса страницы, заданной по умолчанию. Например, при настроенном ha-кластере, в качестве адреса по умолчанию устанавливается адрес ha-кластера.

7) Выполнить настройку **Графического киоска Fly** для профиля **algont**:

– перейти в **Панель управления → Безопасность → Политика безопасности**

– в открывшемся окне в левой панели выбрать **Пользователи → algont** (рисунок 2);

– перейти во вкладку **Графический киоск Fly**;

– активировать параметр **Режим графического киоска Fly**;

– выбрать **Режим одного приложения**, нажать на кнопку внизу вкладки, выбрать скрипт firefox.sh;

– нажать кнопку **Применить изменения**;

8) Войти в ОС под учетной записью пользователя **algont** и убедиться, что автоматически запустился Firefox.

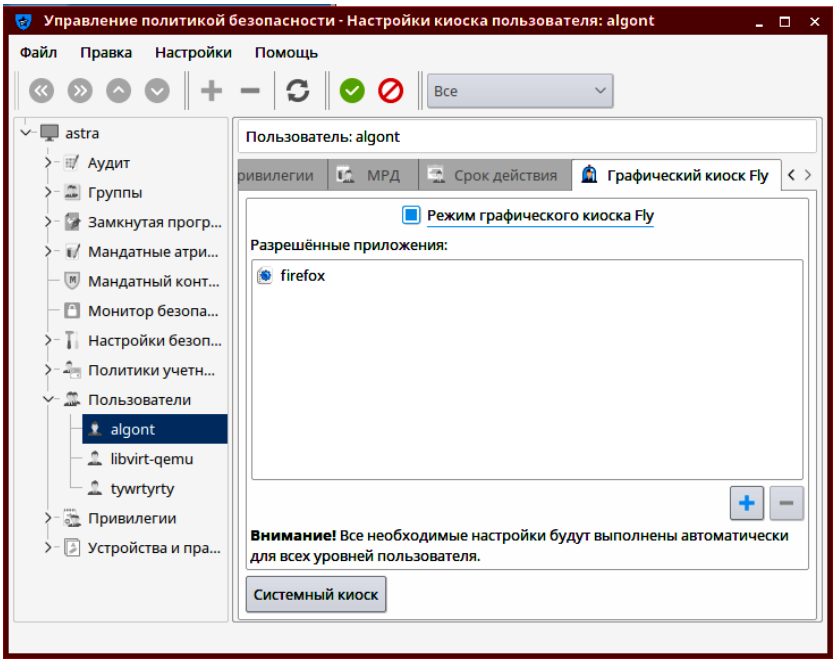

Рисунок 2 — Настройка **Графического киоска Fly** для профиля algont

При необходимости повторить 5)—8) для пользователя ОС с другим именем.

2.3 Скрытие адресной панели Firefox

Перед выполнением действий, описанных ниже, необходимо хотя бы один раз зайти в систему под пользователем оператора АРМ, чтобы запустился firefox и создался профиль пользователя firefox.

1. Перейдите в каталог профиля браузера Mozilla Firefox. Как правило, название каталога для созданного по- умолчанию профиля оканчивается на **default-release**

   cd /home/USER/.mozilla/firefox/PROFILE-NAME

   Обратите внимание:

   – **USER** - имя пользователя, для которого осуществляется операции
   – **PROFILE-NAME -** имя каталога с профилем браузера Mozilla Firefox
2. Включите поддержку загрузки сторонних стилей интерфейса браузера, добавив строку

   user_pref("toolkit.lega- cyUserProfileCustomizations.stylesheets", true); в файл prefs.js:

   echo 'user_pref("toolkit.legacyUserProfileCustomizations.stylesheets", true);' >> prefs.js
3. Создайте директорию **chrome:**

   mkdir chrome
4. Создайте файл **userChrome.css** со следующим содержанием:

   #nav-bar, #identity-box, #tabbrowser-tabs, #TabsToolbar {visibility: collapse !important;}
5. Файл **userChrome.css** может быть создан с помощью следующей команды:

   echo '#nav-bar, #identity-box, #tabbrowser-tabs, #TabsToolbar {visibility:collapse !important;}' >> chrome/userChrome.css

В результате выполненых действий браузер Mozilla Firefox будет запускаться без элементов управления.

2.4 Настройка политик браузера Firefox

1. Перейдите в каталог установки браузера Mozilla Firefox:
   `cd /usr/lib/firefox`
2. Создайте директорию **distribution**, если она отсутствует**:**
   `mkdir distribution`
3. Создайте файл **policies.json** со следующим содержанием:

```
{
  "policies": {
    "BlockAboutAddons": true,
    "BlockAboutProfiles": true,
    "BlockAboutSupport": true,
    "DisableDeveloperTools": true,
    "DisableFirefoxAccounts": true,
    "DisableFormHistory": true,
    "DisplayMenuBar": "never",
    "BlockAboutConfig": true,
    "DisableAppUpdate": true,
    "DisableTelemetry": true,
    "DisableFirefoxStudies": true,
    "AppAutoUpdate": false,
    "NewTabPage": false,
    "NetworkPrediction": false,
    "ExtensionUpdate": false,
    "DisplayBookmarksToolbar": false,
    "FirefoxHome": {
      "Search": false,
      "TopSites": false,
      "Highlights": false,
      "Pocket": false,
      "Snippets": false,
      "Locked": false
    },
    "Preferences": {
      "accessibility.force_disabled": {
        "Value": 1,
        "Status": "locked"
      },
      "browser.tabs.warnOnClose": {
        "Value": false,
        "Status": "locked"
      },
      "browser.gesture.pinch.in": {
        "Value": "",
        "Status": "locked"
      },
      "browser.gesture.pinch.in.shift": {
        "Value": "",
        "Status": "locked"
      },
      "browser.gesture.pinch.out": {
        "Value": "",
        "Status": "locked"
      },
      "browser.gesture.pinch.out.shift": {
        "Value": "",
        "Status": "locked"
      },
      "browser.gesture.swipe.down": {
```

```
            "Value": "",
            "Status": "locked"
          },
          "browser.gesture.swipe.left": {
            "Value": "",
            "Status": "locked"
          },
          "browser.gesture.swipe.right": {
            "Value": "",
            "Status": "locked"
          },
          "browser.gesture.swipe.up": {
            "Value": "",
            "Status": "locked"
          },
          "browser.gesture.tap": {
            "Value": "",
            "Status": "locked"
          },
          "browser.gesture.twist.end": {
            "Value": "",
            "Status": "locked"
          },
          "browser.gesture.twist.left": {
            "Value": "",
            "Status": "locked"
          },
          "browser.gesture.twist.right": {
            "Value": "",
            "Status": "locked"
          },
          "signon.rememberSignons": {
            "Value": false,
            "Status": "locked"
          },
          "signon.autofillForms": {
            "Value": false,
            "Status": "locked"
          },
          "security.insecure_field_warning.contextual.enabled": {
            "Value": false,
            "Status": "locked"
          }
        }
      }
    }
```


2.5 Изменение пароля пользователя ОС

Изменение пароля пользователя ОС выполняется следующим образом:

– войти в ОС под учетной записью пользователя root;

– в эмуляторе терминала выполнить команду установки пароля passwd. Например, команда установки пароля пользователя algont:

```
passwd algont
```

– ввести новый пароль.

К паролям учетных записей пользователей ОС должен применяться установленный порядок формирования и смены пароля, а также порядок ознакомления, обеспечивающие его конфиденциальность.

Администратор безопасности после установки и первичной настройки программы должен задать новый пароль суперпользователя root:

– в эмуляторе терминала выполнить команду установки пароля:

```
sudo passwd root
```

– ввести новый пароль суперпользователя root.

В дальнейшем учетную запись root может использовать только администратор безопасности для переустановки или обновления СПО «АССаД-ID», запуска скриптов архивации и восстановления БД. Оператор АРМ не должен использовать учетную запись root для работы с СПО «АССаД-ID».

Суперпользователь root имеет право на выполнение всех без исключения операций в ОС. Не храните в открытом виде пароль пользователя root. При утере пароля пользователя root необходима переустановка ОС и СПО.

2.6 Отключение нежелательных протоколов и служб

Для предотвращения возможности загрузки вредоносного кода на веб-сервер Apache Tomcat через пользовательский файл необходимо отключить протокол Apache JServ Protocol. Отключение протокола AJP на всех серверах и станциях распознавания выполнить следующим образом:

– войти в ОС под учетной записью пользователя root;

– из конфигурационного файла /assad-id/tomcat/conf/server.xml удалить строку:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"/>
```

Для предотвращения возможности удаленного подключения к серверу или станции распознавания с неавторизованного рабочего места необходимо отключить автозапуск служб Bluetooth, OpenVPN, Samba, SMTP, SSH на всех серверах и станциях распознавания следующим образом:

– войти в ОС под учетной записью пользователя root;

– в эмуляторе терминала выполнить команды:

```
service bluetooth stop
service nmbd stop
service smbd stop
service smtp stop
service ssh stop
service openvpn stop
update-rc.d bluetooth remove
update-rc.d nmbd remove
update-rc.d smbd remove
update-rc.d smtp remove
update-rc.d ssh remove
update-rc.d openvpn remove
```

2.7 Изменение критически значимых паролей

В настоящем пункте приведено описание процедуры по изменению паролей, которые могут быть подвергнуты вредоносной деятельности с целью осуществления деструктивного программного воздействия на систему.

К паролям учетных записей пользователей, приведенных далее, должен применяться установленный порядок формирования и смены пароля, а также порядок ознакомления, обеспечивающие его конфиденциальность.

Особые требования предъявляются к паролям учетных записей пользователей Apache Tomcat в связи с осознанием масштаба деструктивного воздействия в случае их раскрытия. Помимо соответствия общим требованиям, настоятельно рекомендуется устанавливать данные пароли длиной не менее 12 символов.

Последовательность действий по изменению паролей представлена в таблице 1.

Таблица 1 — Параметры профиля пользователя

№ п/п	Последовательность действий	Место выполнения		
		осн. сервер	рез. сервер	ст. расп.
1.	Остановить СПО «АССаД-ID», выполнив команду `service assadid stop`	●	●	●
2.	В файле /assad-id/tomcat/conf/tomcat-users.xml в следующей строке заменить значение полей **password** и **username**: `<user password="password" roles="tomcat, manager,manager-gui,manager-text,manager-script,admin-gui" username="username" />` Примечание — данный логин и пароль используется в административной панели Tomcat	●	●	●
3.	В файле /assad-id/tomcat/webapps/ha/META-INF/tomcat-users.xml в следующей строке заменить значение полей **password** и **name**: `<user name=" name" password="password" roles="hamanager" />` Примечание — данный логин и пароль используется в панели настройки ha-кластера	●	●	-
4.	В файле /assad-id/tomcat/webapps/repl/META-INF/tomcat-users.xml в следующей строке заменить значение полей **password** и **name**: `<user name="name" password="password" roles="replmanager" />` Примечание — данный логин и пароль используется в панели настройки сервиса репликации.	●	●	-

5.	Выполнить следующие команды для замены значений полей **password** (оставив одинарные кавычки) в терминале под учетной записью root:
	`psql -q -d bioxid -U BIOXID -c "ALTER ROLE \"ASSAD_REPL\" WITH SUPERUSER INHERIT NOCREATEDB NOCREATEROLE LOGIN UNENCRYPTED PASSWORD 'ПАРОЛЬ ДЛЯ РОЛИ ASSAD_REPL';"`
	`psql -q -d bioxid -U BIOXID -c "ALTER ROLE \"BIOXID\" WITH SUPERUSER INHERIT CREATEROLE CREATEDB LOGIN UNENCRYPTED PASSWORD 'ПАРОЛЬ ДЛЯ РОЛИ BIOXID';"`
		●	●	-

6.	В файле /assad-id/tomcat/webapps/BioxidServer/ META-INF/context.xml в следующей строке заменить значение поля **connectionPassword** на пароль для роли **BIOXID**, установленный ранее в п.7: `connectionName="BIOXID" connectionPassword= "ПАРОЛЬ ДЛЯ РОЛИ BIOXID"` В файле /assad-id/tomcat/webapps/BioxidServer/ WEB-INF/classes/hibernate.cfg.xml в следующей строке заменить значение поля **connection.password** на пароль для роли	●	●	-

№ п/п	Последовательность действий	Место выполнения		
		осн. сервер	рез. сервер	ст. расп.
	BIOXID, установленный ранее в п.7: <property name="connection.password"> **ПАРОЛЬ ДЛЯ РОЛИ BIOXID**</property> В файле /assad-id/tomcat/webapps/repl/WEB-INF/replicator.xml в следующей строке заменить значение атрибута **value** на пароль для роли **ASSAD_REPL**, установленный ранее в п.7: <property property="password" value= **"ПАРОЛЬ ДЛЯ РОЛИ ASSAD_REPL"**/> В файле /assad-id/tomcat/webapps/BioxidArchive/ WEB-INF/classes/replicator.xml в следующей строке заменить значение поля **connection.password** на пароль для роли **BIOXID**, установленный ранее в п.7: <property name="connection.password"> **ПАРОЛЬ ДЛЯ РОЛИ BIOXID**</property>			
7.	В файле /assad-id/tomcat/webapps/BioxidControl/META-INF/context.xml в следующей строке заменить значение поля **connectionPassword** на пароль для роли **BIOXID**, установленный ранее в п.7: <Realm className="org.apache.catalina.realm.JDBCRealm" connectionName="BIOXID" connectionPassword=**"ПАРОЛЬ ДЛЯ РОЛИ BIOXID"** В файле /assad-id/tomcat/webapps/BioxidControl/WEB-INF/classes/hibernate.cfg.xml в следующей строке заменить значение поля **connection.password** на пароль для роли **BIOXID**, установленный ранее в п.7: <property name="connection.password">**ПАРОЛЬ ДЛЯ РОЛИ BIOXID**</property>	-	-	●
8.	В файле /assad-id/tomcat/webapps/BioxidCheck/WEB-INF/classes/hibernate.cfg.xml в следующей строке заменить значение поля **connection.password** на пароль для роли **BIOXID**, установленный ранее в п.7: <property name="connection.password">**ПАРОЛЬ ДЛЯ РОЛИ BIOXID**</property>	●	●	●
9.	Запустить СПО «АССаД-ID», выполнив команду service assadid start	●	●	●

ВНИМАНИЕ! ПРОЦЕДУРА ПО ИЗМЕНЕНИЮ ПАРОЛЕЙ ДОЛЖНА ВЫПОЛНЯТЬСЯ НА ВСЕХ СЕРВЕРАХ И СТАНЦИЯХ РАСПОЗНАВАНИЯ. ДЛЯ ОБЕСПЕЧЕНИЯ БЕСПЕРЕБОЙНОГО ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ПАРОЛИ ДОЛЖНЫ БЫТЬ ИДЕНТИЧНЫ НА ВСЕХ УСТРОЙСТВАХ.

3 РЕАЛИЗАЦИЯ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

3.1 Организация доступа к системе

Пользователем является непосредственный клиент биометрической системы, управляющий и использующий биометрические приложения, но не взаимодействующий непосредственно с биометрической системой.

Аутентификация пользователя в СПО «АССаД-ID» производится по логину и паролю.

За формирование пользовательского веб-интерфейса СПО «АССаД-ID» отвечает СПО сервера «АССаД-ID».

Доступ пользователей к информации является авторизованным. Для каждого пользователя устанавливается пароль доступа к веб-серверу, установленному на сервере «АССаД-ID».

Получить доступ к веб-интерфейсу СПО «АССаД-ID» может только зарегистрированный пользователь.

При установке пароля в СПО «АССаД-ID» производится проверка соответствия пароля следующим минимальным требованиям качества:

– минимальная длина пароля — 8 символов;

– пароль должен содержать латинские прописные и строчные символы, цифры и специальные символы;

– при изменении пароля он должен отличаться как минимум тремя символами от 24 предыдущих паролей пользователя;

Для каждого пароля устанавливается срок действия (по умолчанию — 1 месяц).

Полномочия пользователя для доступа к отдельным объектам системы определяются ролью, выданной пользователю: администратор безопасности, системный администратор, менеджер по персоналу, построитель отчетов, гость.

Для каждой роли заданы доступные методы и пункты меню. Роли не доступны для редактирования. Пункты меню, доступные пользователям с различными ролями, приведены в табл. 3.

3.2 Контроль над действиями пользователей

Полномочия пользователя для доступа к отдельным объектам системы определяются ролью, выданной пользователю.

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

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. 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

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

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

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

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

Событие «Выход из системы» регистрируется при нажатии кнопки «Выход» в пользовательском интерфейсе или через 30 минут бездействия (если в течение часа оператор не выполняет никаких действий, например, навигация по страницам, изменение параметров и т. п.).

При аварийной ситуации или технической необходимости оператор АРМ «АССаД-ID» может завершить сеанс пользователя ОС с помощью клавиатурного сочетания **Alt+F4.** После завершения сеанса на экране отображается стартовое окно ОС, на котором можно выбрать такие действия как отключение компьютера или перезагрузка.

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

3.3 Контроль доступа к стойке

Для контроля доступа к компьютерному оборудованию системы «АССаД-ID» используется ИБП, оснащенный платой сетевого управления (Network Management Card), стандарта SNMP, поддерживающей подключение внешних датчиков. Например: APC NMC AP9616, AP9617, AP9618, AP9630, AP9810.

К вводу 1 типа «сухой контакт» карты сетевого управления подключается датчик вскрытия стойки (шкафа), в которой размещено компьютерное оборудование, или датчик двери в помещение, в котором размещено компьютерное оборудование.

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

ИБП размещается в стойке вместе с компьютерным оборудованием.

4 КОНТРОЛЬ ЦЕЛОСТНОСТИ

4.1 Общие сведения

Для автоматизированного архивирования и восстановления БД используются скрипты из каталога dbbackup.

Дублирование БД на разных компьютерах в реальном времени выполняет веб-приложение repl.

Описание архивирования и восстановления БД, настройки репликации БД приведено в руководстве системного программиста ЦРПА.2.00067.01.00 32.

Тестирование СЗИ выполняется с помощью веб-приложения auth-test.

Контроль целостности файлов по эталонным контрольным суммам выполняется средствами ОС.

Описание проверки контрольных сумм и тестирование СЗИ приведено ниже.

4.2 Автоматический и автоматизированный контроль целостности файлов

СПО «АССаД-ID» обеспечивает автоматический (ежедневный) и автоматизированный (по команде оператора) контроль целостности СЗИ, входящих в его состав. При проверке СЗИ выполняется расчет контрольных сумм предопределенного списка файлов и производится сравнение полученных значений со значениями, хранящимися в БД. Расчет контрольных сумм производится с использованием алгоритма ГОСТ Р 34.11-2012 256 бит с помощью программы gostsum из состава операционной системы специального назначения Astra Linux Special Edition (не ниже очередного обновления версии 1.7).

По результату сравнения сервера и станции распознавания формируют события «Проверка контрольных сумм прошла успешно» (если значения совпадают) или «Проверка контрольных сумм прошла с ошибками» (если значения не совпадают).

Проверка контрольных сумм автоматически запускается при старте сервера и станции распознавания.

Проверка контрольных сумм ежедневно выполняется в указанное в параметре «Время ежедневной проверки» на всех серверах и станциях распознавания, которые в данный момент обслуживаются.

Ручной запуск проверки контрольных сумм выполняется пользователем с ролью «Администратор безопасности» с помощью кнопки «Проверить контрольные суммы» из меню пользовательского интерфейса «Настройки» → «Оборудование» → «Серверы» и «Станции распознавания». Результатом ручной проверки является список контролируемых файлов и полученных значений контрольных сумм. Если проверка контрольных сумм прошла с ошибками, указывается поврежденный файл.

Контрольные суммы файлов СЗИ приведены в файле gostsumsIST.txt, размещённом на установочном диске и обновлениях изделия.

4.3 Тестирование СЗИ

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

Для тестирования работы СЗИ необходимо выполнить следующие действия:

1) перейти по ссылке http://[IP-адрес]:8080/auth-test, где IP-адрес — IP-адрес компьютера сервера «АССаД-ID»;

2) ввести логин и пароль администратора безопасности;

3) нажать кнопку «Начать тестирование».

При запуске тестирования происходит автоматический выход из системы текущего оператора.

В процессе тестирования автоматически выполняются следующие операции:

– авторизация администратора безопасности;
– создание пользователя (с ролью «Гость»);
– выход администратора безопасности из системы;
– авторизация пользователя;
– попытка доступа к разрешенным данным (попытка перехода на страницу «Абоненты»);
– попытка доступа к запрещенным данным (попытка перехода на страницу «Пользователи»);
– выход пользователя из системы;
– авторизация администратора безопасности;
– удаление пользователя;
– выход администратора безопасности из системы.

В процессе выполнения операций на экране отображаются выполняемые действия.

При попытке несанкционированного доступа к странице отображается сообщение «Доступ к странице запрещен».

5 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ОПЕРАТОРОВ

Пользователем (оператором) является непосредственный клиент биометрической системы, управляющий и использующий биометрические приложения, но не взаимодействующий непосредственно с биометрической системой.

Получить доступ к веб-интерфейсу СПО «АССаД-ID» может только зарегистрированный пользователь СПО «АССаД-ID».

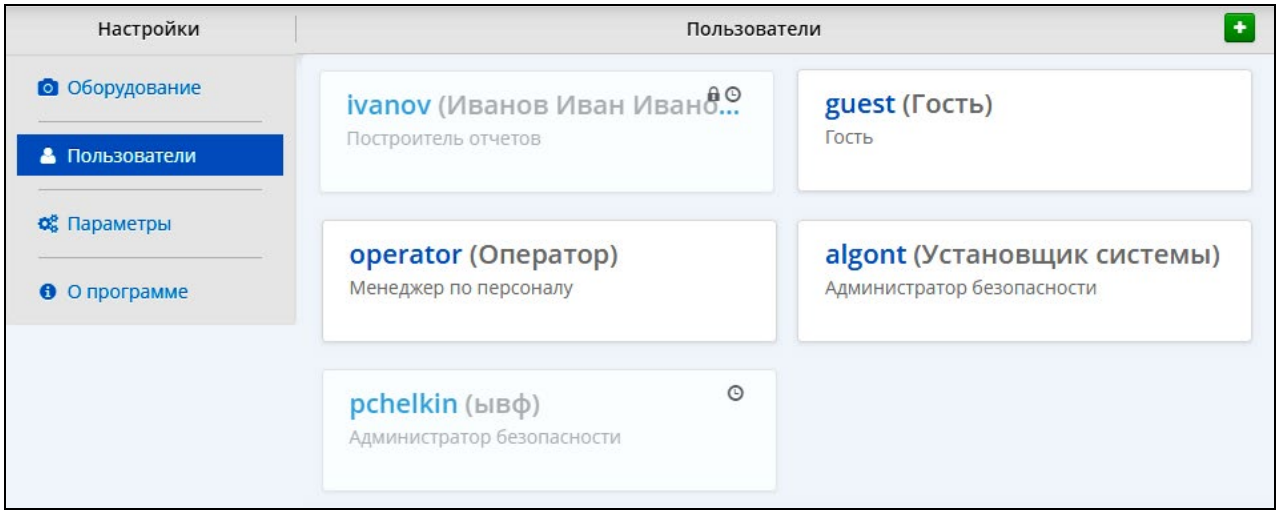

Рисунок 3 - Пользователи

Индикаторы (рисунок 3) учетной записи пользователя:

Срок действия пароля истек, вход в систему невозможен, требуется смена пароля или продление срока его действия.

Пользователь заблокирован.

По умолчанию после установки в системе доступен единственный пользователь с логином algont, паролем algont и правами администратора безопасности.

Пользователь algont является системным, его нельзя удалить, изменить его логин или уровень доступа. Для редактирования доступен только пароль. Наличие пользователя algont необходимо для обмена информацией между службами, входящими в состав системы.

После первого входа в систему пароль пользователя algont необходимо сменить.

ВНИМАНИЕ! ПОСЛЕ СМЕНЫ ПАРОЛЯ ПОЛЬЗОВАТЕЛЯ algont ДОЛЖНА БЫТЬ ВЫПОЛНЕНА ПЕРЕЗАГРУЗКА ВСЕХ СЕРВЕРОВ И СТАНЦИЙ РАСПОЗНАВАНИЯ.

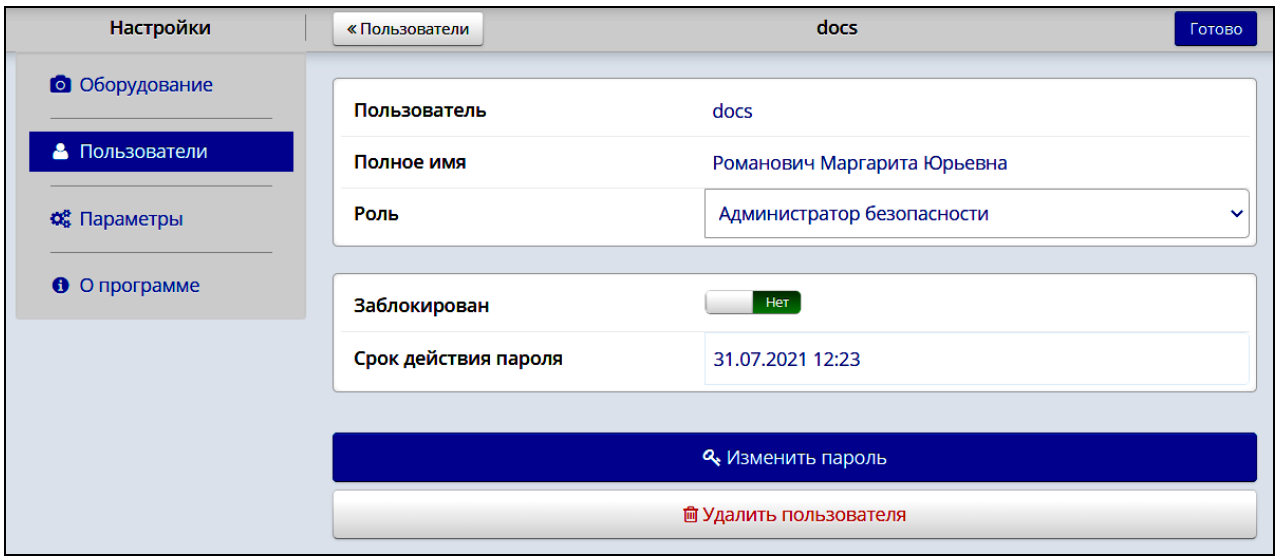

Рисунок 4 — Страница конфигурации профиля пользователя

Описание доступных параметров профиля пользователя (рисунок 4) представлено в таблице 2.

Таблица 2 — Параметры профиля пользователя

Параметр	Описание
Пользователь	Логин (имя) пользователя. Используется для входа в систему. Логин является уникальным идентификатором, добавление двух пользователей с одинаковым логином невозможно
Полное имя	Полное имя пользователя или его описание
Роль	Уровень доступа пользователя. Описания уровней доступа пользователей различных типов представлено в таблице 3.
Заблокирован	Пользователь может быть заблокирован пользователем системы с правами администратора безопасности.
Срок действия пароля	По истечению срока действия пароля вход в систему будет невозможен.

Поля **Логин**, **Пароль** и **Подтверждение** являются обязательными для заполнения.

Изменение пароля пользователя выполняется нажатием на кнопку **Изменить пароль**.

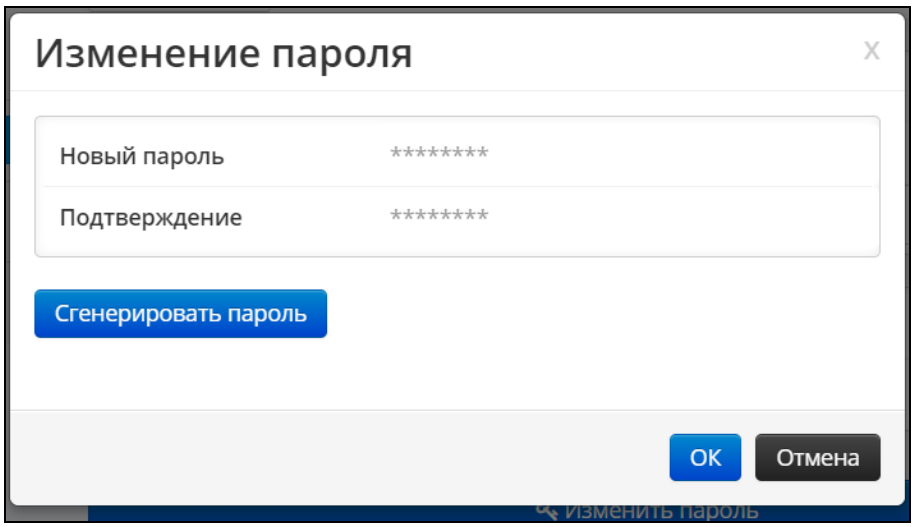

Рисунок 5 — Изменение пароля

Для автоматической генерации пароля, удовлетворяющего требованиям безопасности, необходимо нажать на кнопку **Сгенерировать пароль** (рисунок 5).

При вводе пароля вручную для исключения возможной ошибки ввода запрашивается его подтверждение.

Таблица 3 — Роли пользователей

Роль	Описание	Доступные пункты меню
Администратор безопасности	Полный доступ ко всем данным системы: добавление, изменение, удаление информации об абонентах, настройка (параметры системы, пользователи, серверы, станции распознавания и т. д.), формирование любых отчетов.	Абоненты Отчеты Настройки
Системный администратор	Полный доступ, за исключением доступа к аудиту пользователей, построения отчета о безопасности и проверки контрольных сумм.	Абоненты Отчеты (кроме отчетов о безопасности) Настройки (кроме пользователей и проверки контрольных сумм)
Менеджер по персоналу	Пользователь может добавлять, изменять, удалять данные об абонентах, формировать отчеты о распознавании и аналитические отчеты.	Абоненты Отчеты (только аналитика и о распознавании)
Построитель отчетов	Просмотр информации об абонентах и формирование отчетов о распознавании.	Абоненты (только просмотр) Отчеты (только аналитика и о распознавании)
Гость	Только просмотр информации об абонентах.	Абоненты (только просмотр)

6 РЕГИСТРАЦИЯ СОБЫТИЙ

6.1 Общие сведения

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

6.2 Уведомления

Для пользователей с правами системного администратора и администратора безопасности формируется список сообщений, требующих внимания (рисунок 6). Из списка уведомлений можно удалить ⊗ отдельные события, или очистить список полностью с помощью кнопки **Очистить все**.

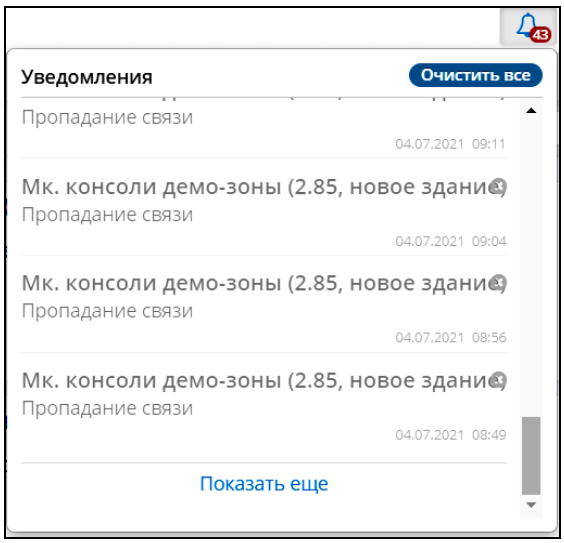

Рисунок 6 — Список сообщений

Администратор безопасности информации получает следующие уведомления:

– «Стойка открыта»;
– «Отказано в доступе»;
– «Проверка контрольных сумм прошла с ошибками»;
– «Пропадание связи».

Сообщения, потерявшие актуальность, выделяются серым. Например, если после события пропадания связи с устройством было зарегистрировано событие появления связи, событие считается неактуальным.

6.3 Отчеты

На странице **Отчеты** формируются отчетные документы на основе событий, зафиксированных в журнале событий системы за выбранный период.

Сформированный в виде таблицы отчет можно распечатать, сохранить как файл в формате *.csv.

Доступ к отчетам разного типа определяется ролью пользователя.

Таблица 4 — Типы отчетов

Тип	Описание
Аналитика	Графики на основе событий о распознавании абонентов.
Безопасность	Сообщения о доступе пользователя и его действиях. Позволяет контролировать действия оператора: вход в систему, выход из системы, просмотр, добавление, изменение или удаление данных в конфигурации системы.
Распознавание	Сообщения о распознавании абонентов.
Системный	Сообщения оборудования.

Максимальный период, за который можно сформировать отчет — 31 день.

Таблица 5 — Периоды формирования отчета

Период	Описание
За сегодня	С 00:00:00 текущей даты по текущее время.
За вчера	С 00:00:00 по 23:59:59 даты, предшествующей текущей.
За неделю	Отчет за предшествующие 7 дней (с 00:00:00 по 23:59:59) и текущий день (с 00:00:00 по текущее время).
За месяц	Окончание периода — текущая дата и время. Начало периода — 00:00:00 текущего числа прошлого месяца. Например, отчет **За месяц**, сформированный 22 февраля в 12:35:40, будет включать в себя все события с 00:00:00 22 января по 12:35:40 22 февраля.
За период…	Отчет за произвольный период времени (но не более месяца), начиная с выбранной даты и времени и заканчивая выбранной датой и временем.

Таблица 6 — События отчета о безопасности

Сообщение	Источник	Описание
Отказано в доступе	Сервер	Неудачная попытка входа в пользовательский интерфейс. Возможны следующие причины: – неизвестный пользователь; – неверный пароль; – пользователь заблокирован; – истек срок действия пароля.
Проверка контрольных сумм прошла успешно	Станция распознавания или сервер	Рассчитанные суммы файлов совпадают с контрольными образцами.
Проверка контрольных сумм прошла с ошибками	Станция распознавания или сервер	Рассчитанные суммы файлов не совпадают с контрольными образцами.
Стойка открыта	Станция распознавания или сервер	Стойка с оборудованием «АССаД-ID» была открыта.
Стойка закрыта	Станция распознавания или сервер	Стойка с оборудованием «АССаД-ID» была закрыта.

Сообщение	Источник	Описание
Назначение роли пользователю	Сервер	Изменение роли пользователя.
Изъятие роли пользователя	Сервер	
Просмотр данных	Сервер	Пользователь открыл страницу с параметрами одного из элементов системы (например, параметры консоли).
Удаление данных	Сервер	Из базы данных удален элемент системы (например, удален абонент).
Добавление данных	Сервер	Создан новый элемент системы (например, профиль абонента).
Редактирование данных	Сервер	Изменены один или несколько параметров элемента системы (например, изменен биошаблон абонента).
Установлено обновление	Сервер	Обновлена версия СПО «АССаД-ID».
Разные версии компонентов системы	Сервер	Версия СПО «АССаД-ID» на сервере (источник события) и версия СПО на другом сервере и/или станции распознавания не совпадают. Периодическое сообщение. Проверяется соответствие версий на серверах и станциях распознавания, находящихся на связи.
Одинаковые версии компонентов системы	Сервер	Версия СПО «АССаД-ID» на сервере (источник события) и версия СПО на всех остальных серверах и станциях распознавания совпадают. Периодическое сообщение. Проверяется соответствие версий на серверах и станциях распознавания, находящихся на связи.
Вход в систему	Сервер	Пользователь подключился к серверу «АССаД-ID» с помощью веб-интерфейса.
Выход из системы	Сервер	Оператор вышел из веб-интерфейса Событие формируется только в том случае, если пользователь нажал для выхода.

Сообщения отказа в доступе пользователя, неудачной проверки контрольных сумм и открытия стойки выделяются цветом (рисунок 7) и добавляются в список уведомлений.

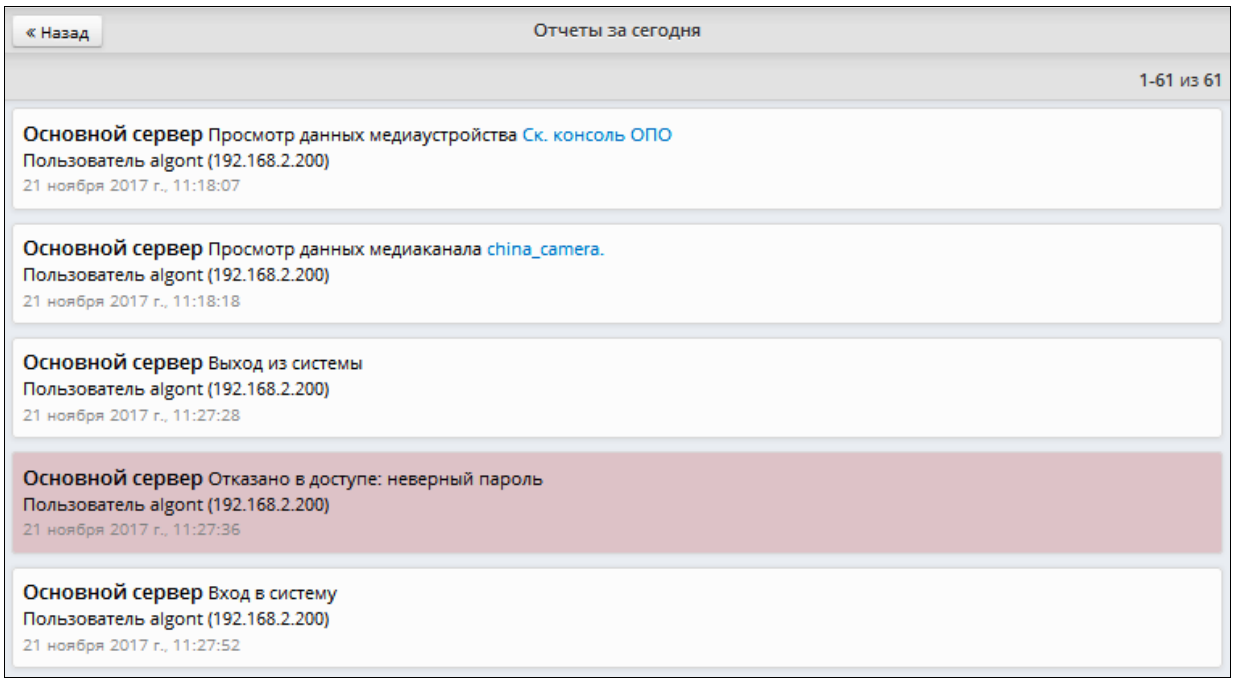

Рисунок 7 — Отчет о безопасности

6.4 Архивация событий

СПО «АССаД-ID» обеспечивает периодическую архивацию событий системы.

Параметры архивации событий определены в файле /assad-id/tomcat/webapps/BioxidArchive/WEB-INF/classes/archive.properties. Описание параметров приведено в таблице 7.

Таблица 7 — Параметры архивации событий

Параметр	Описание	Возможные значения
archiveFolder	Путь к каталогу, в который будут помещаться ZIP-файлы с архивами. Имя архива формируется на базе текущей даты.	/assad-id/archives
autoArchiveDate	Архивация событий будет проводиться каждый месяц в указанный день месяца. Если сервер был отключен в указанный день, то архивация будет произведена на следующий день во время, указанное в параметрах autoArchiveHour и autoArchiveMinute. По умолчанию архивация проводится на следующий день после старта сервера, и в дальнейшем — по первым числам каждого месяца.	–1 (по умолчанию), от 1 до 31
autoArchiveHour	Час и минута, когда будет запускаться архивация в день, определенный параметром autoArchiveDate.	От 0 до 23 По умолчанию — 1
autoArchiveMinute		От 0 до 59 По умолчанию — 0
autoArchiveOnStartup	Признак запуска архивации при каждом старте сервера.	true — архивировать false (по умолчанию) — не архивировать

Параметр	Описание	Возможные значения
eventStoreMonths	Все события, не старше указанного количества месяцев, будут оставлены в БД после завершения архивации. Более старые события удаляются.	По умолчанию — 3
imagesFolder	Путь к каталогу хранения изображений, захваченных в процессе распознавания. Каждое изображение связано с событием распознавания.	/assad-id/tomcat/webapps/BioxidControl/images
imagesStoreMonths	Все изображения, не старше указанного количества месяцев, будут оставлены в БД после завершения архивации. Более старые изображения удаляются.	По умолчанию — 4
imagesDeleteDelay	Все изображения (за исключением изображений не старше imagesStoreMonths) будут удалены из БД через указанное количество часов после удаления событий. Задержка между удалением событий и связанных с событиями изображений необходима при архивации на нескольких серверах.	По умолчанию — 24

7 СООБЩЕНИЯ АДМИНИСТРАТОРУ БЕЗОПАСНОСТИ

Сообщения администратору безопасности отображаются в уведомлениях (см. п. 6.2) и в отчете о безопасности (см. 6.3).

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					
8	-	все	-	-	27	ЦРПА.0067-24			