Описание функциональных характеристик ПК BOT-Trek TDS

Программный комплекс Bot-Trek TDS является средством защиты конфиденциальной информации (системой обнаружения вторжений уровня сети) и предназначен для автоматизированного обнаружения компьютерных атак (вторжений) и вредоносного ПО в сетевом трафике при помощи сигнатурного метода выявления атак и эвристического анализа. Изделие устанавливается на границе сети с целью повышения уровня защищенности ИС, ЦОД, серверов и коммуникационного оборудования, АРМ пользователей.

Сигнатурный анализ трафика выполняется программным комплексом в соответствии с регулярно обновляемым классификатором угроз, созданным на основе лучших мировых практик реагирования на инциденты информационной безопасности, расследований, экспертиз. Источником данных для классификатора являются не только открытые/специализированные Интернет-ресурсы, но и результаты работы подразделений разработчика изделия в указанных выше видах деятельности.

Эвристический анализ трафика выполняется в соответствии с собственной базой правил анализа и выявления аномалий в сетевом трафике.

Программный комплекс Bot-Trek TDS детектирует следующие вторжения – Trojan-Activity, Банковские трояны (Banking), POS-трояны (POS), APT-трояны, Бэкдор-трояны (Backdoor), Нежелательное ПО (Unwanted), Связка эксплойтов (EK), Подозрительная активность (Suspicious), DDoS-трояны, Программы-вымогатели (Ransomware).

Изделие ПК Bot-Trek TDS прошло сертификационные испытания на соответствие требованиям документов: Требования к Системам обнаружения вторжений, Профиль защиты СОВ (уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ). Сертификат № 3850 от 5 ноября 2019 года.

В ПК Bot-Trek TDS реализованы следующие функции безопасности системы обнаружения вторжений (СОВ):

1) разграничение доступа к управлению системой обнаружения вторжений;
2) управление работой системы обнаружения вторжений;
3) управление параметрами системы обнаружения вторжений;
4) управление установкой обновлений (актуализации) базы решающих правил системы обнаружения вторжений;
5) анализ данных системы обнаружения вторжений;
6) аудит безопасности системы обнаружения вторжений;

7) контроль целостности системы обнаружения вторжений;

8) сбор данных о событиях и активности в контролируемой информационной системе;

9) реагирование системы обнаружения вторжений;

10) идентификация и аутентификация.

ПК Bot-Trek TDS обеспечивает следующие функциональные возможности:

- сбор информации о сетевом трафике;
- анализ собранных данных системы обнаружения вторжений о сетевом трафике в режиме, близком к реальному масштабу времени, и по результатам анализа фиксация информации о дате и времени, результате анализа, идентификаторе источника данных, протоколе, используемом для проведения вторжения;
- анализ собранных данных с целью обнаружения вторжений с использованием сигнатурного и эвристических методов;
- анализ собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика на заданном уровне эвристического анализа;
- обнаружение вторжений на основе анализа служебной информации протоколов сетевого уровня базовой эталонной модели взаимосвязи открытых систем;
- фиксация факта обнаружения вторжений или нарушений безопасности в журналах аудита;
- уведомление администратора системы обнаружения вторжений об обнаруженных вторжениях по отношению к контролируемым узлам ИС и нарушениях безопасности с помощью отображения соответствующего сообщения (пиктограммы) в графическом интерфейсе;
- автоматизированное обновление базы решающих правил;
- тестирование (самотестирование) функций безопасности изделия (контроль целостности исполняемого кода изделия);
- управление режимом выполнения функций безопасности изделия со стороны уполномоченных администраторов (ролей);
- управление данными изделия со стороны уполномоченных администраторов (ролей);
- поддержка определенных ролей для изделия и их ассоциации с конкретными администраторами СОВ и пользователями ИС;

- администрирование изделия;
- генерация записей аудита для событий, потенциально подвергаемых аудиту;
- ассоциация каждого события аудита с идентификатором субъекта, его инициировавшего;
- предоставление возможности читать информацию из записей аудита;
- ограничение доступа к чтению записей аудита;
- поиск, сортировка, фильтрация данных аудита.

В основу функционирования сетевого сенсора (сетевого датчика) ПК Bot-Trek TDS положен сигнатурный и эвристический метод выявления атак. Он обеспечивает обнаружение атак на основе специальных шаблонов (сигнатур) и эвристических правил, каждое из которых соответствует конкретной атаке. При получении исходных данных о сетевом трафике автоматизированной информационной системы ПК Bot-Trek TDS производит их анализ на соответствие указанным шаблонам атак, имеющихся в базе данных.

В случае обнаружения сигнатуры или отработки правила в исходных данных изделие регистрирует факт обнаружения атаки, оповещает администратора безопасности о данном событии. За счет использования механизма контроля целостности ПК Bot-Trek TDS позволяет отслеживать действия нарушителя по отношению к контролируемым ресурсам в скомпрометированной системе. Дополнительно поддерживается получение данных о функционировании отдельных объектов контролируемой системы по используемым приложениям в протоколах верхнего уровня (браузеры, почтовые клиенты).

ПК Bot-Trek TDS реализует следующие методы реагирования на факт выявления компьютерной атаки:

- идентификация компьютерной атаки с использованием описаний уязвимостей, на которые они направлены, или описаний реализаций компьютерных атак;
- оповещение администратора безопасности об обнаруженных атаках;
- регистрация атаки в журнале аудита ПК Bot-Trek TDS.

ПК Bot-Trek TDS имеет текстовую консоль, которая реализует механизм локального управления данным средством обнаружения атак и позволяющий: производить настройку своих компонентов, их запуск, остановку и перезапуск. Связь между удаленной текстовой консолью и компонентом изделия, выполняющим управление сетевым оборудованием,

осуществляется по отдельно выделенному сетевому интерфейсу. Изделие позволяет в автоматическом режиме получать новые сообщения от датчиков для системных журналов контролируемой системы.

С целью маскирования изделия в составе контролируемой системы предполагается выделение изделия в отдельный сегмент, если на защищаемых объектах не установлены датчики контроля целостности, или отделение компонентов изделия от возможных нарушителей с помощью межсетевых экранов, исключая точки съема информации сетевыми датчиками. В качестве дополнительной меры по затруднению демаскирования компонентов изделия предусмотрена возможность наложения ограничений на сетевые адреса, между которыми осуществляется взаимодействие компонентов.

ПК Bot-Trek TDS реализует следующие механизмы собственной защиты:

- обеспечивается идентификация и аутентификация администратора при запуске текстовой консоли по имени пользователя и паролю; ведется контроль длины создаваемых паролей (не менее 8 символов) и состав паролей (буквенно-цифровые);
- в процессе работы осуществляется контроль целостности компонентов и конфигурации изделия;
- имеет функцию сигнализации администратору безопасности о неверных попытках аутентификации при доступе к изделию, в частности, сигнализации о трех подряд неверных попытках аутентификации путем записи соответствующего события в системный журнал.

Изделие регистрирует в своих журналах аудита следующие события:

- сведения о выявленных компьютерных атаках и случаях нарушения целостности контролируемых ресурсов;
- сведения о сообщениях системных журналов с машин контролируемых ресурсов;
- служебную информацию, формируемую компонентами изделия, такую как подключение или отключение компонентов изделия, вход и выход администратора.

Дополнительные характеристики изделия:

- имеет механизм фильтрации событий, отображаемых в журналах;
- обладает интуитивно-понятным русскоязычным графическим интерфейсом и графическим текстовым интерфейсом администрирования;
- работает под управлением UNIX подобных операционных систем;

– обеспечивает анализ стека протоколов TCP/IP начиная с канального уровня;

– имеет возможность генерации табличных и текстовых отчетов на основе содержимого журналов;

– имеет распределенную модульную архитектуру, обеспечивающую масштабируемость системы, позволяющую адаптироваться под требования конкретной системы по производительности и отказоустойчивости;

– существует возможность резервирования ключевых компонентов.

Структура изделия приведена на рис. 1.

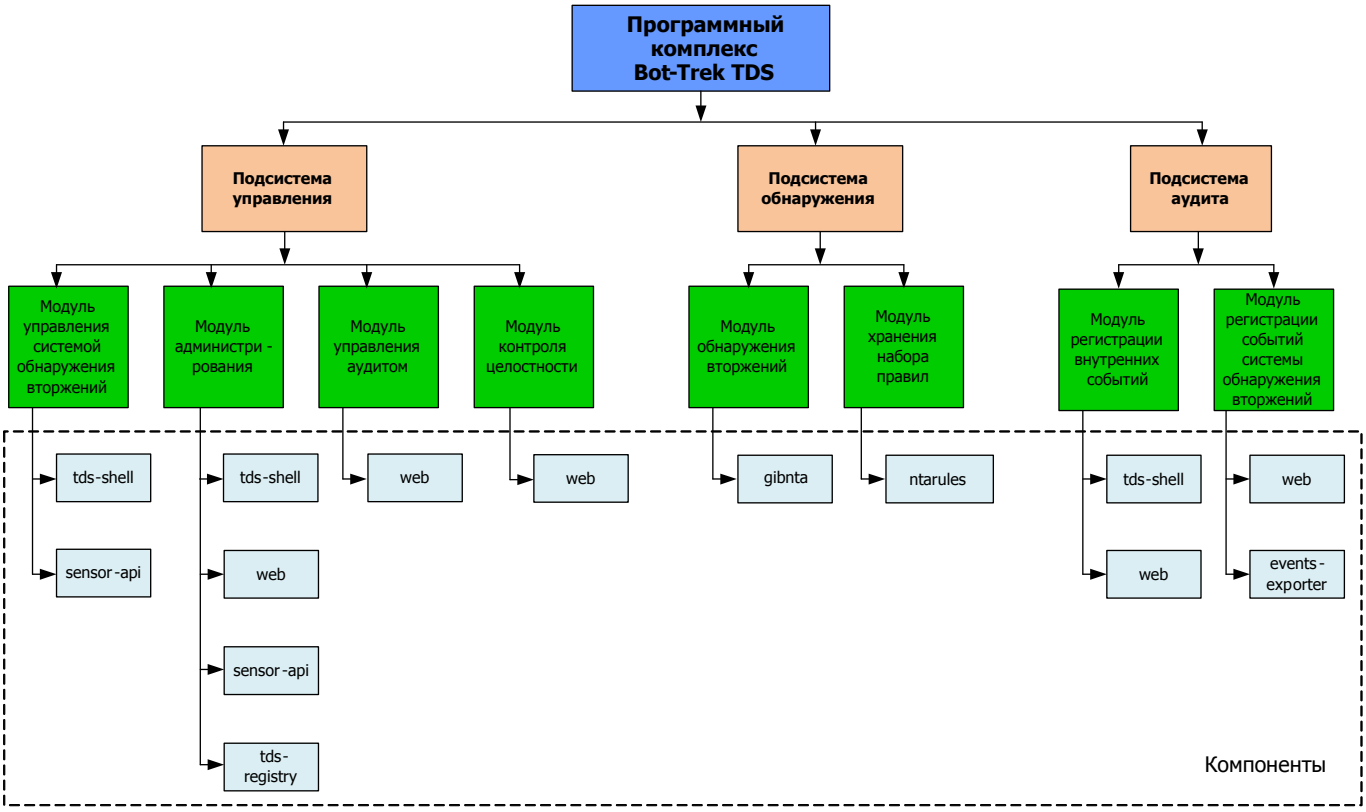

Рис. 1

Описание компонентов изделия приведен ниже:

1) **Gibnta** – сенсор, движок, выполняющий сигнатурный анализ.

2) **ntarules** – база решающих правил (БРП) – централизованное хранение набора правил, предназначенных для эвристического анализа трафика и набор сигнатур для выявления аномальных событий по атакам на защищаемые ресурсы.

3) **tds-shell** – консольная панель управления (текстовая консоль) с псевдографическим интерфейсом для первоначальной настройки.

4) **web** – web-интерфейс, панель администратора и аудит безопасности.

5) **sensor-api** – прослойка для **tds-shell** и **web**. Предоставляет им API для управления и настройки системы.

6) **events-exporter** – компонент «забирающий» события (данные) из **Redis** и «кладущий» их в базу данных (компонент **events-exporter** входит в состав компонента **web**).

7) **tds-registry** – конфигурационный файл и механизм управления им для работы системы в целом.

Работа системы обнаружения вторжений

Работа системы обнаружения вторжений неизменна для всех типов детектируемых угроз.

Описание работы системы обнаружения вторжений приведено на рис. 2.

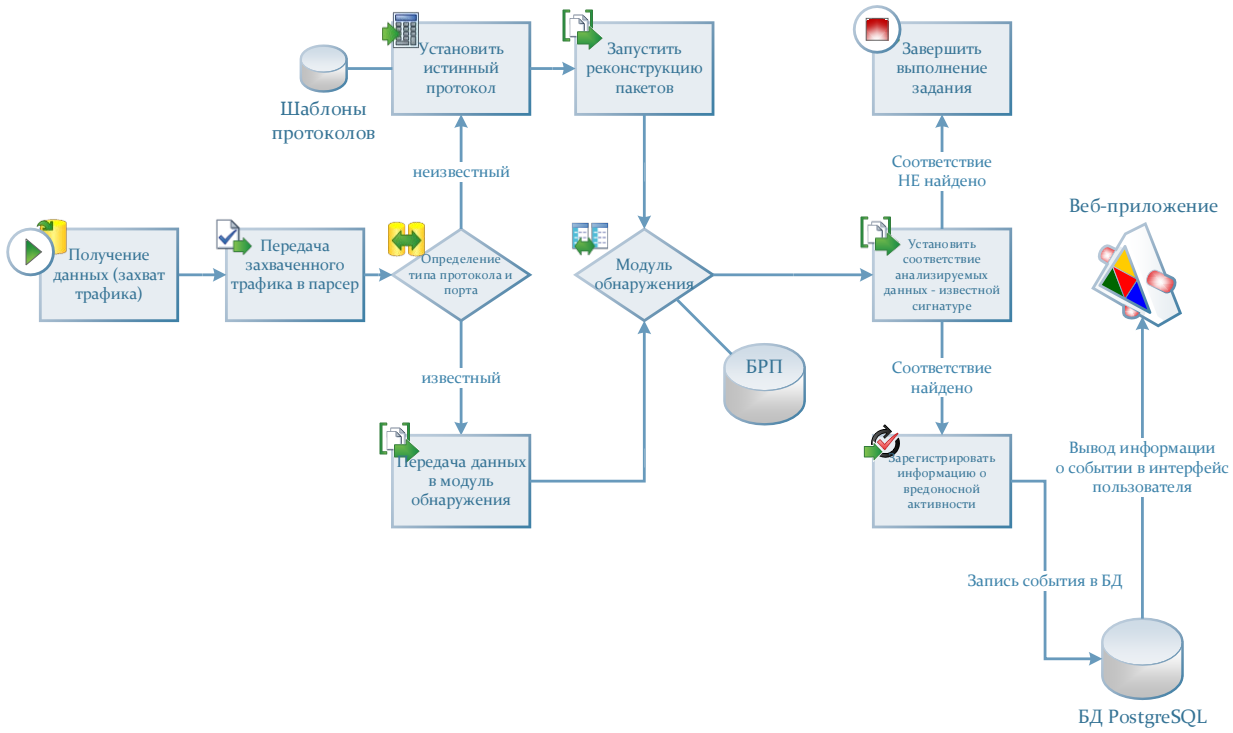

Рис. 2

Система обнаружения вторжений действует по приведенному алгоритму, то есть анализирует поток поступающего на ее вход трафика, при этом входящий трафик разбивается на TCP, UDP или другие транспортные потоки, после чего парсеры пакетов (синтаксические анализаторы) маркируют их и разбивают на высокоуровневые протоколы и их поля – нормализуя, если требуется. Полученные декодированные, раскрытые и нормализованные поля протоколов (пакеты) затем проверяются наборами сигнатур, которые выявляют есть ли среди сетевого трафика попытки сетевых атак или пакеты, присущие вредоносной активности.

Работа модуля обнаружения приведена на рис. 3.

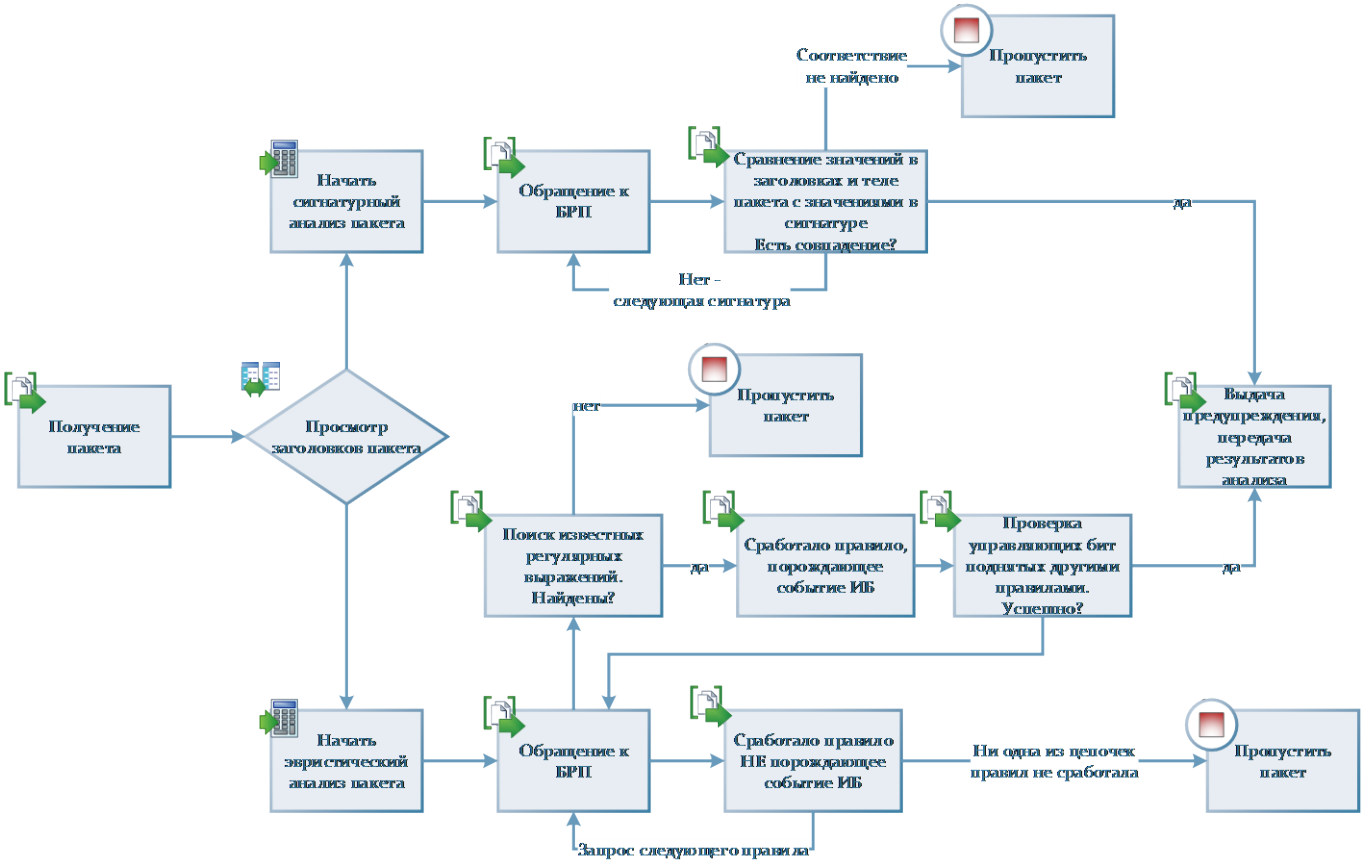

Рис. 3

С получением на вход пакета модуль обнаружения начинает его обработку. Анализируются заголовки пакета, запускаются процессы сигнатурного и эвристического анализа. Сигнатурный анализ характеризуется непрерывным сравнением значений в заголовках и теле пакета с значениями, указанными в сигнатуре. Модуль обнаружения в этом случае будет перебирать сигнатуры из Базы решающих правил до тех пор, пока не будет выявлено соответствие известной сигнатуре, которая относится к тому, или иному классу. Если такого соответствия установлено не будет, модуль пропустит пакет и его анализ на этом завершится.

Анализ пакета эвристическим методом так же начинается с выявления соответствия значений в заголовках и теле пакета наборам эвристических правил, хранящихся в Базе решающих правил. Основным отличием данного метода от сигнатурного является сопоставление значений в заголовках пакета не конкретным сигнатурам, а цепочкам правил, которые делятся на два типа:

- порождающие события;
- не порождающие события.

Каждое из правил может как поднимать управляющие биты (флаги) для анализируемой информации, так и проверять наличие уже поднятых другими правилами флагов.

При этом пакет может пройти проверку несколькими правилами, которые не порождают событий ИБ. В этом случае событие информационной безопасности не будет зафиксировано модулем обнаружения и анализ пакета эвристическим методом завершится.

Если в цепочке правил сработало правило, порождающее событие ИБ, модуль обнаружения производит сопоставление значений в теле пакета известным ему регулярным выражениям и проверяет всю цепочку правил, которые поднимали управляющие биты. При этом управляющие биты могли быть подняты в ходе анализа предыдущих сетевых пакетов. Результатом работы модуля обнаружения в этом случае является выдача предупреждения о событии ИБ и передача данных о сработавших правилах в базу данных.

Такой подход к анализу сетевого трафика позволяет существенно повысить вероятность обнаружения атак (вторжений), распределенных во времени, и в том случае если эксплуатация уязвимости реализуется распределением тела атаки в разных сетевых пакетах хаотично и непоследовательно.

Таким образом модуль обнаружения, используя эвристический метод анализа сетевого трафика, опирается на Базу решающих правил в принятии решения о выдаче предупреждения и регистрации событий информационной безопасности.

На рис. 4 показана последовательность действий при разборе сетевого пакета:

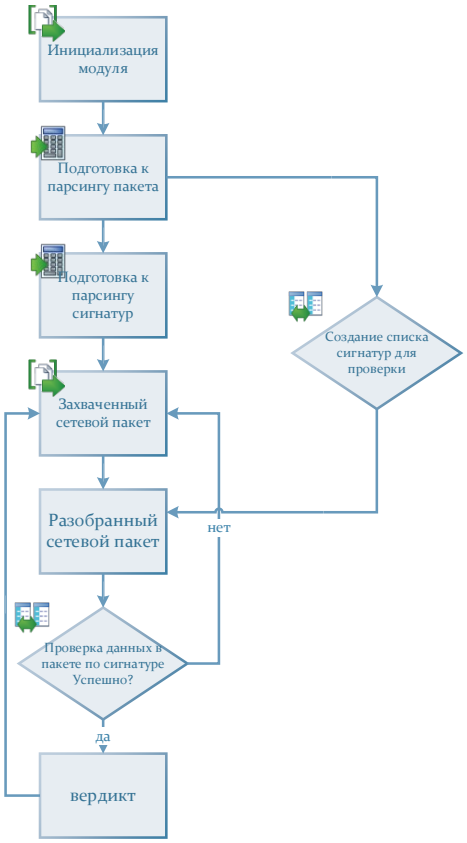

Рис. 4

Каждый сетевой пакет разбирается отдельно, данные из пакета перед проведением анализа сохраняются в структурированном виде. Эта структура с сохраненной информацией, извлеченной из захваченного пакета данных, необходима для последующей процедуры проверки указанных данных по сигнатурам и цепочкам правил.

После завершения парсинга пакетов модуль обнаружения сравнивает результаты анализа с сигнатурами и цепочками правил, чтобы определить, произошло ли вторжение, если будет установлено соответствие, модуль обнаружения вынесет вердикт с указанием сработавшей сигнатуры или цепочки правил.

Успешность сигнатурного и эвристического метода анализа трафика полностью зависит от количества и качества загруженных сигнатур и правил в базу решающих правил. База регулярно обновляется, сигнатуры и правила ежемесячно дополняются, но при этом структура системы обнаружения вторжений и схема ее работы не изменяются.

База решающих правил состоит из множества сигнатур. Сигнатуры по своей сути – это набор данных, на которые опирается сенсор, анализируя трафик. Этот набор данных в большинстве своем берется из тела атаки (файла вредоносного ПО или сетевого пакета, принадлежащего эксплойту). Поэтому классификация сигнатур представляет из себя виды угроз, реализуемые с помощью того или иного вида вредоносного ПО или метода реализации вторжения (атаки) на защищаемую сетевую инфраструктуру.

Выполнение поставленных задач достигается за счет:

– наличия облачного интерфейса – вся информация о выявленных угрозах доступна в веб-интерфейсе, через который удобно отслеживать уведомления в течение дня;

– применения наглядных отчетов – визуализированная статистика по периодам и по типам событий позволяет отслеживать изменения в динамике и характере атак.

Список использованных при разработке ПО сторонних компонентов

При разработке и тестировании программного обеспечения использовался следующий инструментарий:

– компилятор GCC для языков C, C++.

– компилятор g++ языка C++.

– IDE SublimeText с набором плагинов. Плагины включают в себя подсветку и проверку синтаксиса. Синхронизация с системой контроля версия Git.

– текстовый редактор Sublime Text. Поддерживает плагины на языке программирования Python.

– SonarQube — платформа с открытым исходным кодом для непрерывного анализа и измерения качества кода.

– Cppcheck — статический анализатор кода для языка C/C++, предназначенный для поиска ошибок, которые не обнаруживаются компиляторами. Главной целью проекта является сведение до минимума количества ложных срабатываний при поиске ошибок.

– Eslint — это инструмент, который позволяет проводить анализ качества кода, написанного на любом выбранном стандарте JavaScript. Он приводит код к единому стилю, помогает избежать ошибок, умеет автоматически исправлять многие из найденных проблем и хорошо интегрируется со многими инструментами разработки. Для проведения статического анализа JavaScript в составе Eslint использовался плагин ScanJS. который был создан в качестве вспомогательного средства для проверки, чтобы помочь выявить проблемы безопасности в клиентских веб-приложениях. ScanJS использует Acorn - небольшой, быстрый парсер JavaScript, написанный полностью на JavaScript.

– программа фиксации и контроля исходного состояния программного комплекса «ФИКС» (далее - программа «ФИКС», ФИКС), версия 2.0.2 (копия № 5018, знак соответствия № А 278982, сертификат ФСТЭК России № 1548 от 15.01.2008 г., продлен до 15.01.2020 г.).

Установка и эксплуатация программного обеспечения

Среда функционирования ПК Bot-Trek TDS

Изделие функционирует в среде операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (версия 1.6) Релиз «Смоленск» на отдельно выделенном сервере СОВ.

Для функционирования подсистемы аудита и базы данных системы обнаружения вторжений используется СУБД PostgreSQL версия 9.6 (входит в состав операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (версия 1.6) Релиз «Смоленск»).

В целях диверсификации используемого программного обеспечения, включенного в рееср отечественного возможность работы с СУБД, включенной в Единый реестр российских программ для электронных вычислительных машин и баз данных, изделие Bot-Trek TDS может использовать СУБД Postgres PRO Standart версии 10.4.1 (сертификат ФСТЭК России № 3637 от 05.10.2016, реестровый номер ПО 104 от 18 Марта 2016).

Для хранения базы решающих правил используется файловая система ОС «Astra Linux Special Edition».

Для хранения событий, генерируемых сенсором, еще не попавших в базу, используется Redis – сетевое журналируемое хранилище данных типа «ключ - значение» (входит в состав операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (версия 1.6) Релиз «Смоленск»).

Технические средства, на которые устанавливается изделие, должны удовлетворять требованиям, необходимым для загрузки операционной системы.

Для функционирования изделия используется любой совместимый «AMD64» сервер.

Характеристики сервера:

- оперативная память – не менее 8 ГБ;
- жесткий диск – не менее 500 ГБ;
- привод CD/DVD;
- монитор;
- клавиатура;
- манипулятор типа «мышь».

Техническое средство (сервер), на котором установлено изделие, должно быть обеспечено источником бесперебойного питания.

Установка дополнительного программного обеспечения в процессе функционирования изделия является нежелательной.

Техническое средство, на котором установлено изделие, должно размещаться в закрытом отапливаемом и кондиционируемом помещении, снабженным средствами пожарной безопасности.

Физический доступ в помещение, где функционирует изделие, должен быть ограничен.

Доступ к изделию и право работы на нем должны иметь только зарегистрированные пользователи.

Установка ПК Bot-Trek TDS

Перед установкой ПК Bot-Trek TDS необходимо:

- проверить правильность подключения клавиатуры и монитора к серверу;
- проверить наличие CD/DVD привода в составе сервера, в случае отсутствия необходимо подключить переносной CD/DVD привод;
- вставить CD-диск с дистрибутивом изделия в CD/DVD привод;
- нажать комбинацию клавиш <Ctrl+Alt+F2> для перехода в консольный режим и ввести имя и пароль пользователя root.

После ввода данных пользователя root будет предоставлен доступ к командной строке ОС.

Установка ПК Bot-Trek TDS выполняется только с помощью установочного скрипта install.sh, который находится в корне дистрибутива ПК Bot-Trek TDS.

Запуск скрипта необходимо осуществлять под пользователем root.

Для установки изделия выполнить следующие действия:

1) монтировать CD-диск с дистрибутивом;
2) найти на CD-диске с дистрибутивом скрипт install.sh;
3) запустить скрипт install.sh;
4) В процессе установки появится всплывающее окно с подтверждением установки пакетов. Подтвердить установку.

Указания по эксплуатации

При эксплуатации изделия необходимо соблюдать выполнение следующих условий:

– исключение возможности использования изделия для обработки информации, содержащей сведения, составляющие государственную тайну;

– наличие администратора СОВ, отвечающего за правильные настройки изделия;

– при доступе к рабочему месту администратора СОВ должна осуществляться его идентификация и аутентификация;

– сохранение в секрете идентификаторов и паролей на доступ к изделию;

– периодическая смена паролей на доступ к изделию;

– обеспечение физической сохранности изделия и ПЭВМ администратора СОВ путем исключения возможности доступа к ним посторонних лиц;

– ведение на резервных носителях двух копий конфигурации изделия, их периодическое (при необходимости) обновление и проверка целостности;

– периодическое тестирование функций защиты изделия администратором СОВ, включающее контроль правильности настроек безопасности изделия, а также проверку целостности его текущей конфигурации;

– администрирование изделия должно осуществляться с рабочего места, на котором должно быть установлено средство антивирусной защиты с последними обновлениями антивирусных баз;

– каналы управления изделия, расположенные в пределах контролируемой зоны, должны быть защищены организационно-техническими мерами;

– для защиты каналов управления изделия, выходящих за переделы контролируемой зоны, должны применяться методы и средства, устойчивые к пассивному и/или активному прослушиванию сети и сертифицированные в установленном порядке или должен быть запрещен удаленный доступ для администрирования изделия по незащищенным каналам связи;

– должна проводиться периодическая проверка на отсутствие уязвимостей с использованием средств анализа защищенности;

– в изделии запрещается установка программного обеспечения, не входящего в оцененную конфигурацию;

– для администрирования изделия может применяться только роль: «администратор безопасности». Применение иных ролей для администрирования изделия запрещено.

Администрирование изделия

Для администрирования изделия используется графический интерфейс и текстовая консоль.

Администрирование производится на АРМ Администратора, подключенного по отдельно выделенному сетевому интерфейсу к серверу СОВ.

Администрирование сетевых настроек СОВ производится в текстовой консоли.

Администратору доступны следующие функции управления (администрирования) программой:

- управление пользователями;
- управление настройками системы обнаружения вторжения;
- управление настройками получения меток времени по протоколу NTP;
- управление настройками сетевого интерфейса управления;
- управление базой решающих правил;
- управление питанием сервера, на котором установлена программа.

Описание аудита событий

Общие сведения

Вход пользователей СОВ в графический интерфейс программы производится посредством ввода в браузере Интернет IP-адреса изделия. После ввода в адресную строку IP-адреса изделия, полученного в ходе настройки, следует открытие страницы входа в программу (рис. 5).

Рис. 5

Смена пароля

Смена пароля может производиться администратором безопасности для любого пользователя путем переходом на вкладку «Пользователи», выбором нужного пользователя и вводом нового пароля в специальном поле ввода (рис. 6) (после сохранения изменений берется хэш от пароля; сам пароль нигде не хранится в открытом виде).

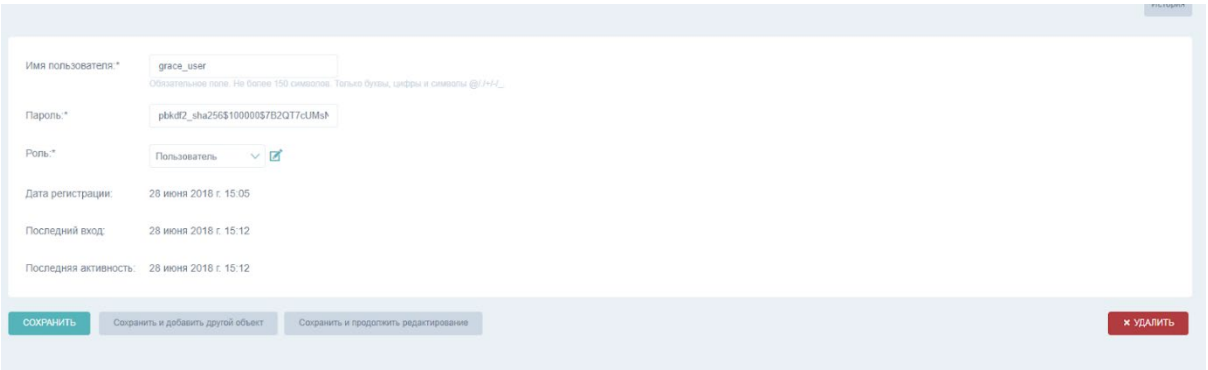

Рис. 6

Смена пароля может производиться любым пользователем для самого себя.

Для этого необходимо нажать на вкладку с именем пользователя в правом верхнем углу главного окна программы, в открывшемся окне нажать на кнопку «Изменить пароль» (рис. 7).

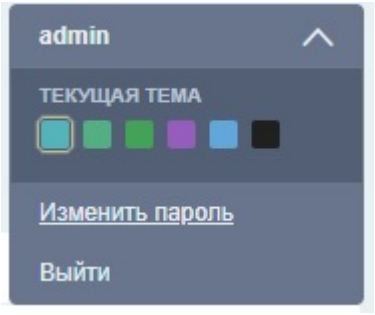

Рис. 7

Произойдет переход на страницу смены пароля, где вводятся соответствующие данные: старый (текущий) пароль, новый пароль, а также подтверждение нового пароля. Введенные данные должны соответствовать специальным требованиям. После совершения этих действий изменения необходимо сохранить (рис. 8).

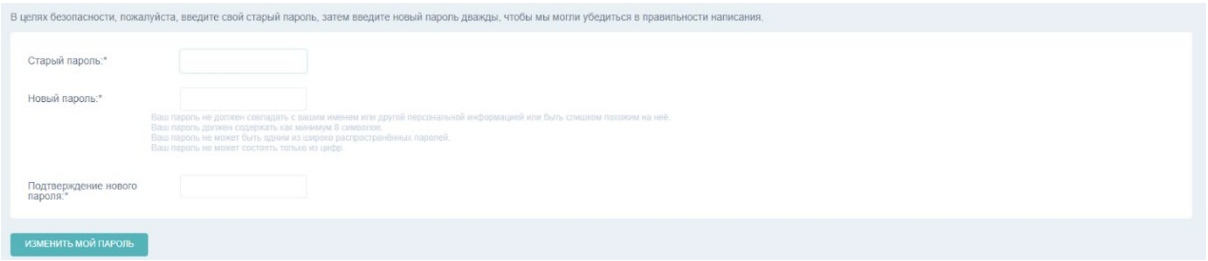

Рис. 8

Создание администратором безопасности нового пользователя

Создание администратором безопасности нового пользователя происходит на вкладке «Пользователи» при помощи нажатия на кнопку [+ Добавить]. Появляется окно в котором необходимо ввести (рис. 9):

– имя пользователя;

– пароль;

– указывается роль (аудитор или пользователь) к которой этот пользователь должен принадлежать.

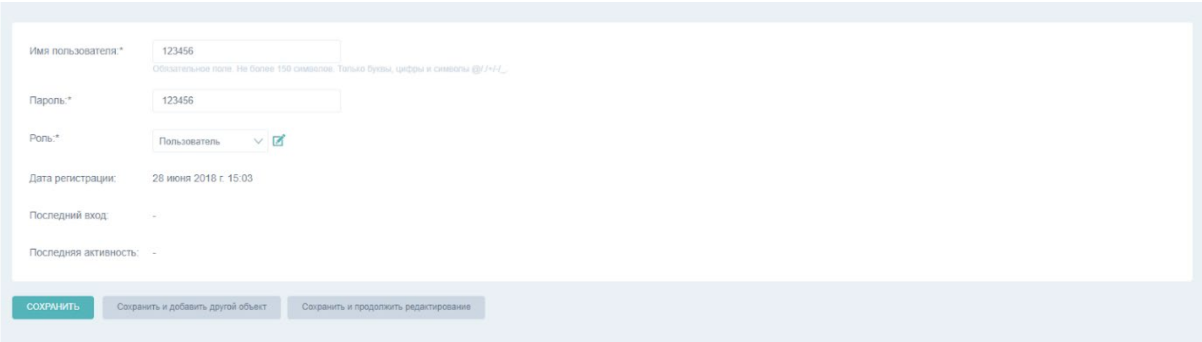

Рис. 9

Главное меню программы

Главное меню программы представляет собой страницу с содержимым, различным для пользователей разных ролей.

Администратору безопасности доступно следующее меню (рис. 10).

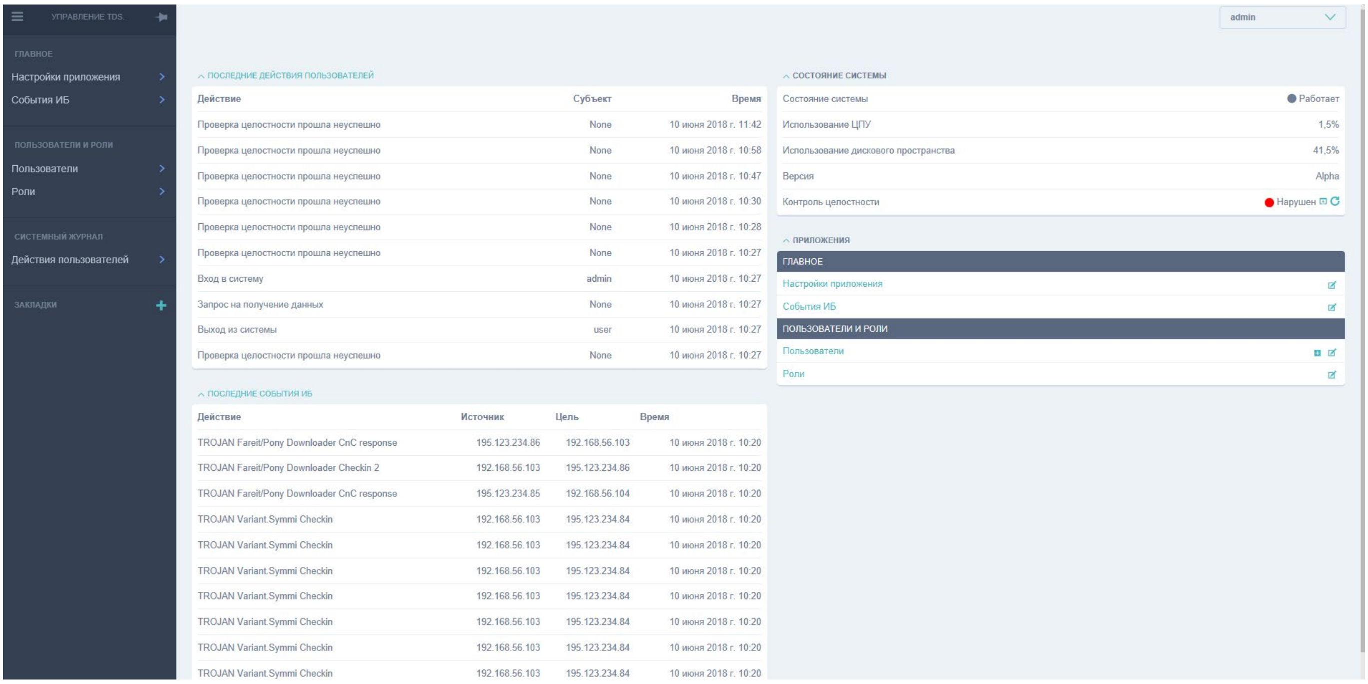

Рис. 10

Администратор безопасности имеет доступ ко всем функциям программы, аудитор просматривает журнал внутренних событий (системный журнал), а пользователь события СОВ.

Окно программы пользователя с ролью Аудитор (рис. 11).

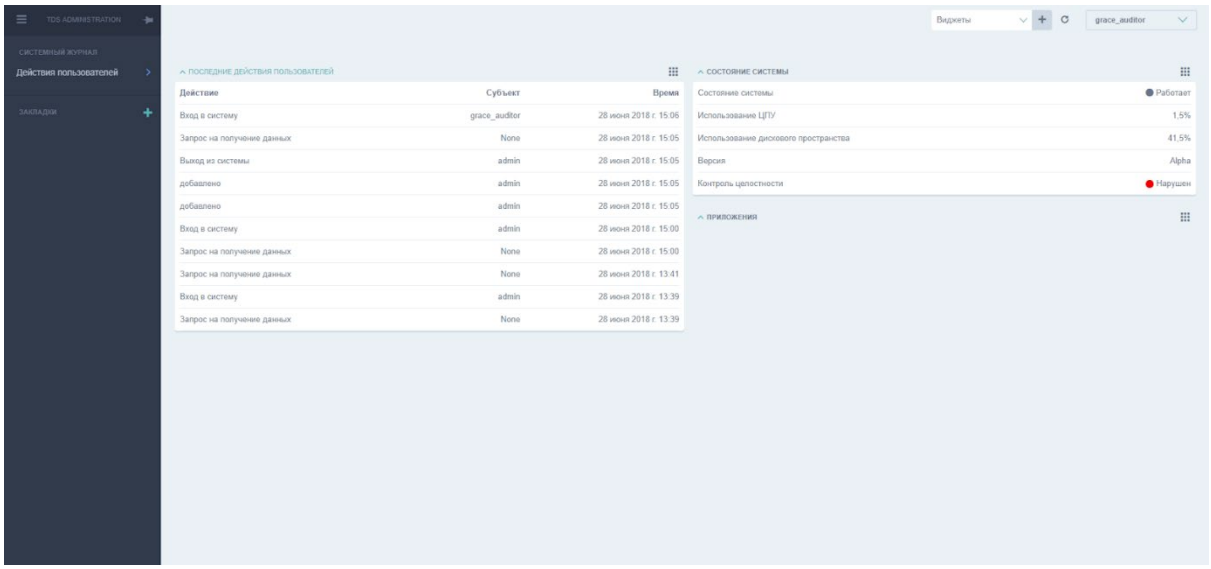

Рис. 11

Пользователю с ролью аудитор доступны функции просмотра системного журнала с действиями пользователей и смены пароля.

Функция «Действия пользователей» предназначена для информирования аудитора о действиях пользователей в режиме реального времени и вывода статистической информации.

Для запуска функции «Действия пользователей» необходимо нажать на вкладку «Действия пользователей» в области «Управление TDS». Откроется окно, как показано на рис. 12.

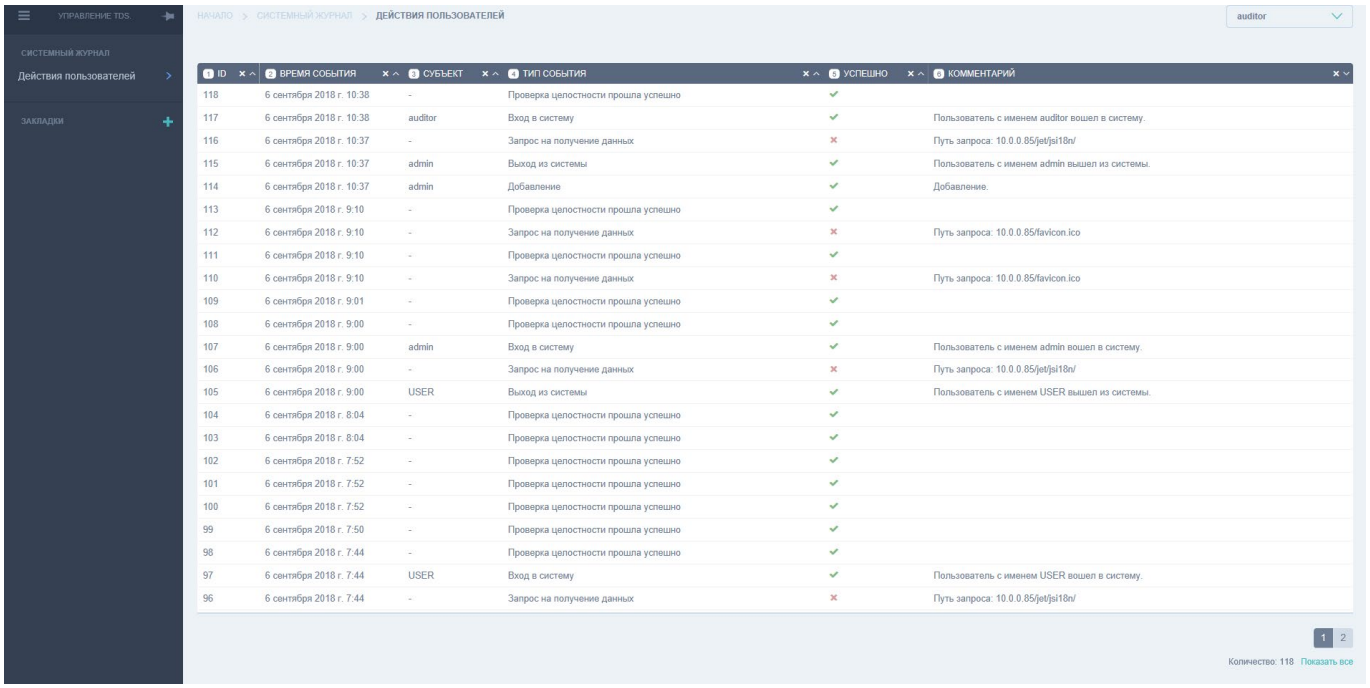

Рис. 12

Для работы аудитору доступна следующая информация о действиях пользователей:

- ID (порядковый номер события);
- Время события (время, когда событие произошло);
- Субъект (пользователь);
- Тип события (вход в систему/выход из системы/запрос на получение данных/добавление/проверка целостности прошла успешно/попытка входа в систему несуществующим пользователем/изменение/запуск функций аудита/остановка функций аудита);
- Успешно (оценка успешности события);
- Комментарий (комментарии действий пользователей).

Окно программы пользователя с ролью Пользователь (рис. 13).

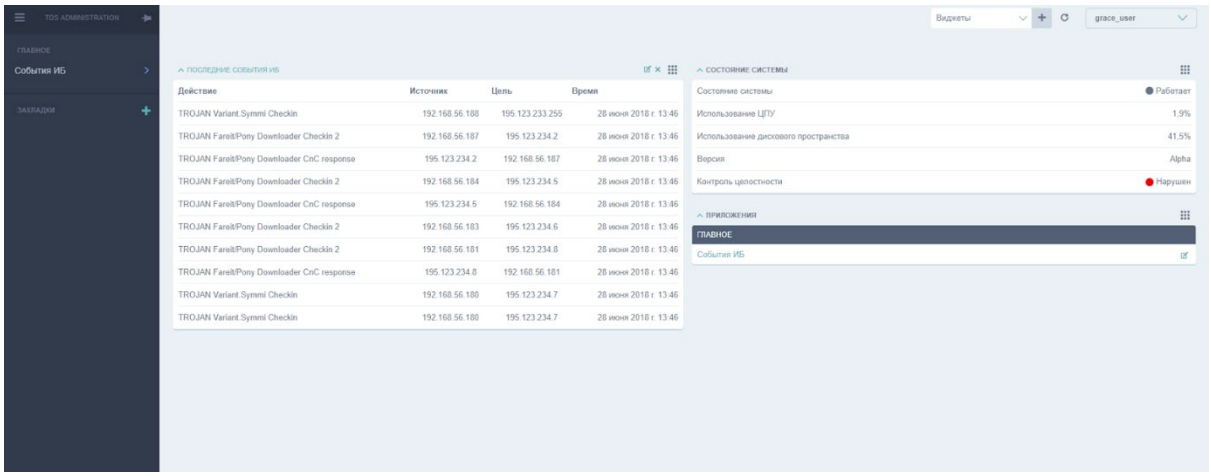

Рис. 13

Описание подсистемы аудита

Подсистема аудита программы реализована на странице «События ИБ».

Главное окно «События ИБ» (рис. 14) содержит следующие поля:

- ID;
- Время события;
- Опасность события;
- Адрес источника;
- Адрес назначения;
- Протокол;
- Сигнатура;
- Содержимое;
- HTTP.

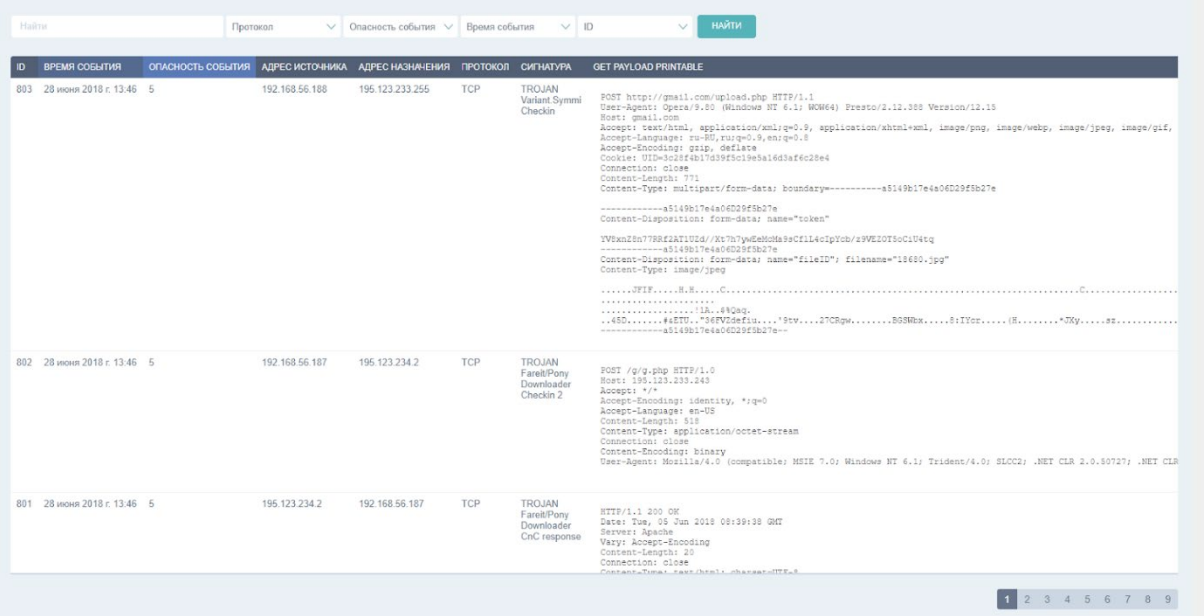

Рис. 14

Поиск событий

Все события отображаются на соответствующей странице «События ИБ».

Доступны следующие функции:

- поиск по ключевым словам в событиях;
- фильтры:
  - по протоколу;
  - опасности события;
  - времени события;
  - ID события.

Оповещения программы

Оповещение осуществляется путем обновления страницы со списком событий ИБ.

Для обновления страницы нажать на клавиатуре клавишу <F5>. Появится значок и поле с описанием как показано на рис. 15.

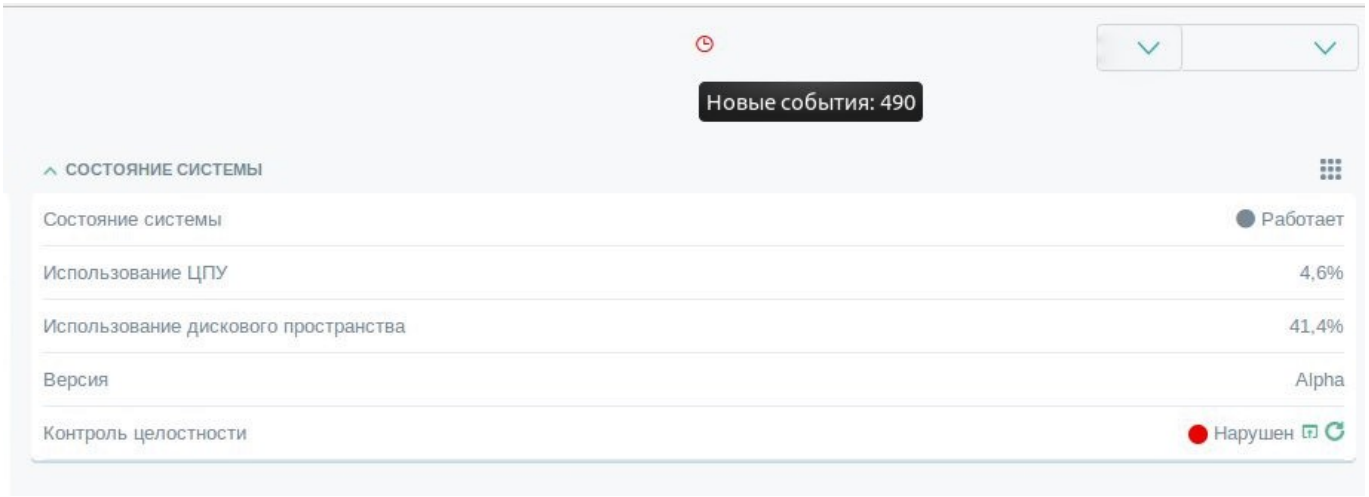

Рис. 15

Контроль целостности

Для выполнения контроля целостности и самотестирования программы администратору безопасности доступно меню «Контроль целостности», которое находится в окне «Состояние системы» (рис. 16).

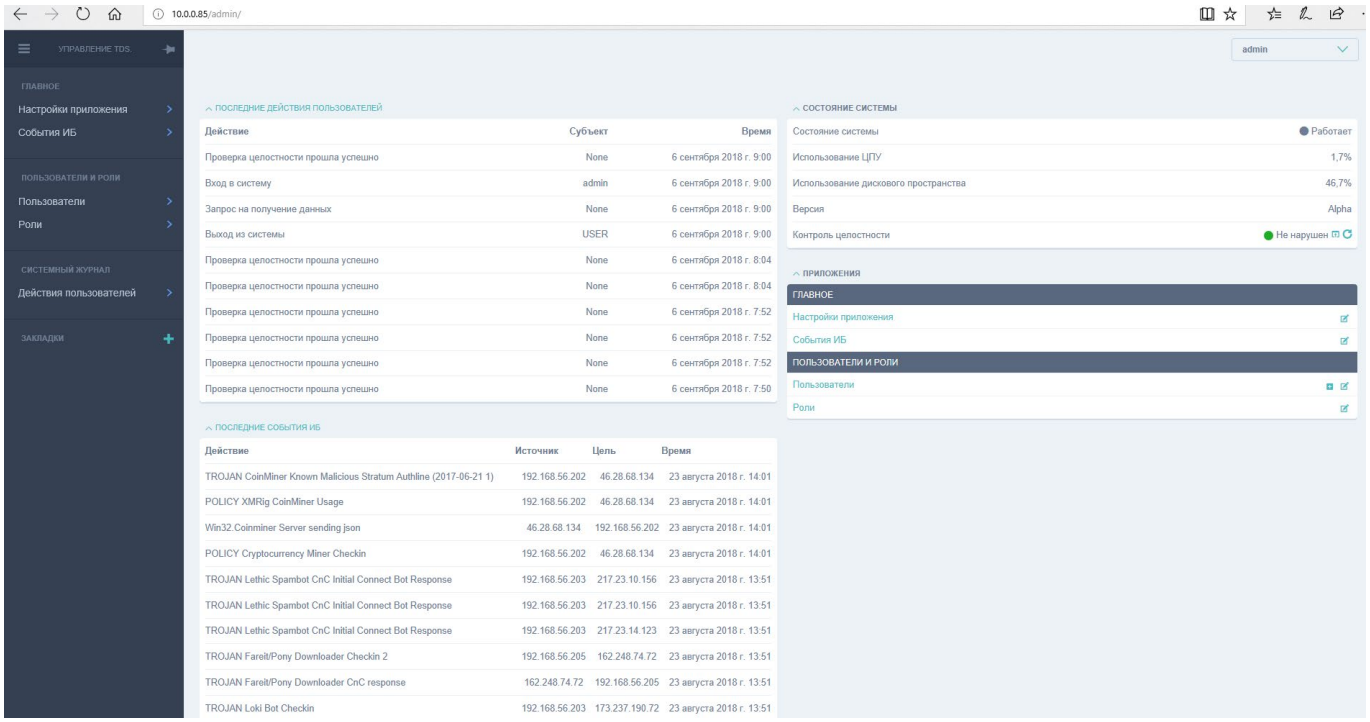

Рис. 16

При нажатии на иконку «Просмотреть» (рис. 17) в окне «Состояние системы» выводится отчет о проверке, как показано на рис. 18.

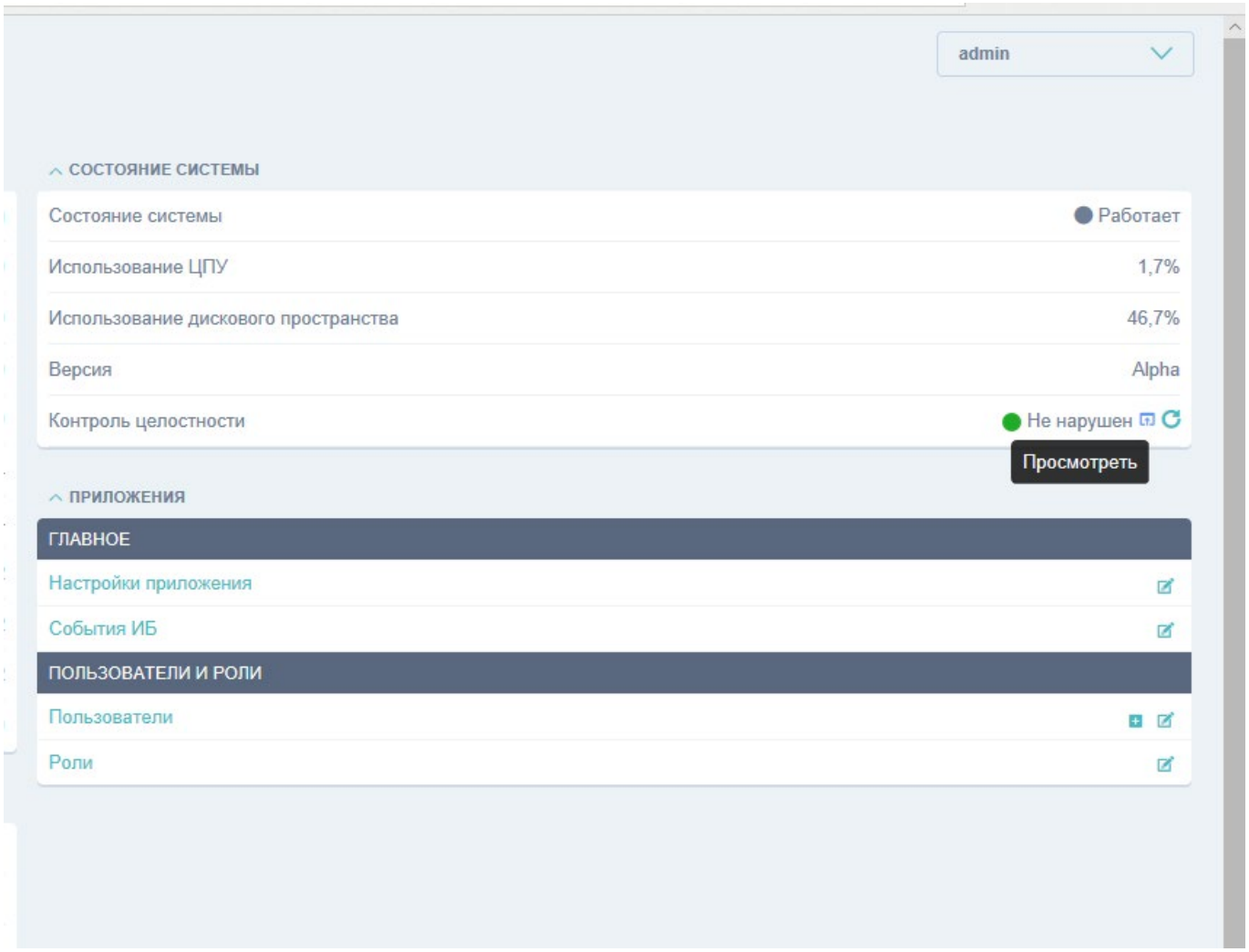
admin
СОСТОЯНИЕ СИСТЕМЫ
Состояние системы
Работает
Использование ЦПУ
1,7%
Использование дискового пространства
46,7%
Версия
Alpha
Контроль целостности
Не нарушен
Просмотреть
ПРИЛОЖЕНИЯ
ГЛАВНОЕ
Настройки приложения
События ИБ
ПОЛЬЗОВАТЕЛИ И РОЛИ
Пользователи
Роли

Рис. 17

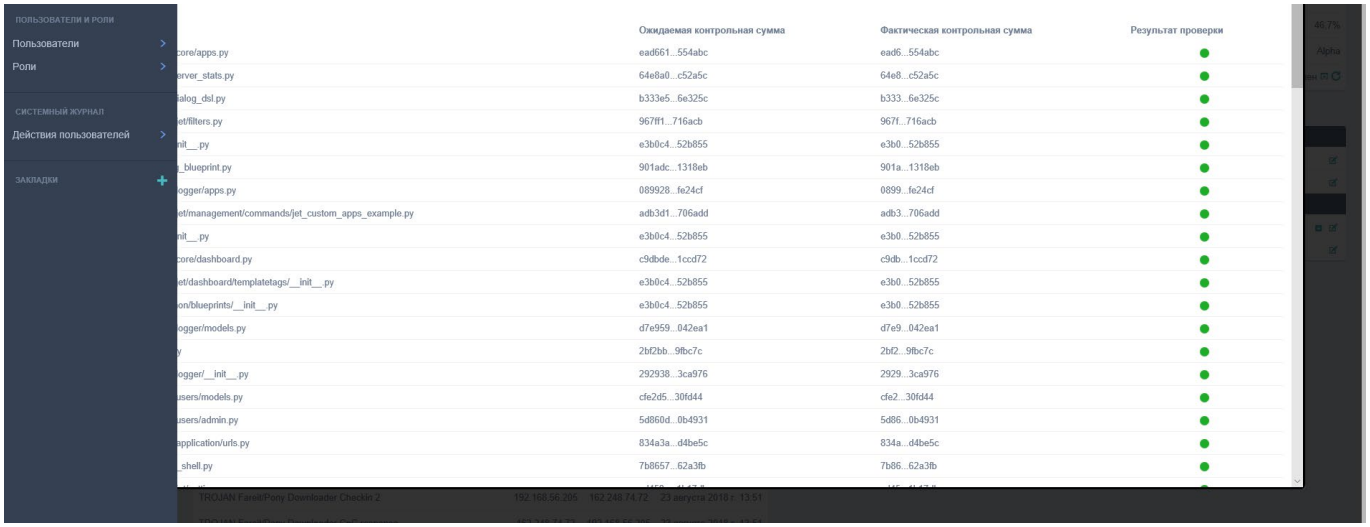
ПОЛЬЗОВАТЕЛИ И РОЛИ
Пользователи
Роли
СИСТЕМНЫЙ ЖУРНАЛ
Действия пользователей
ЗАКЛАДКИ
Ожидаемая контрольная сумма
Фактическая контрольная сумма
Результат проверки

Рис. 18

Обновление данных функции контроля целостности и самотестирования программы производится при нажатии на иконку «Обновить» (рис. 19) в окне «Состояние системы».

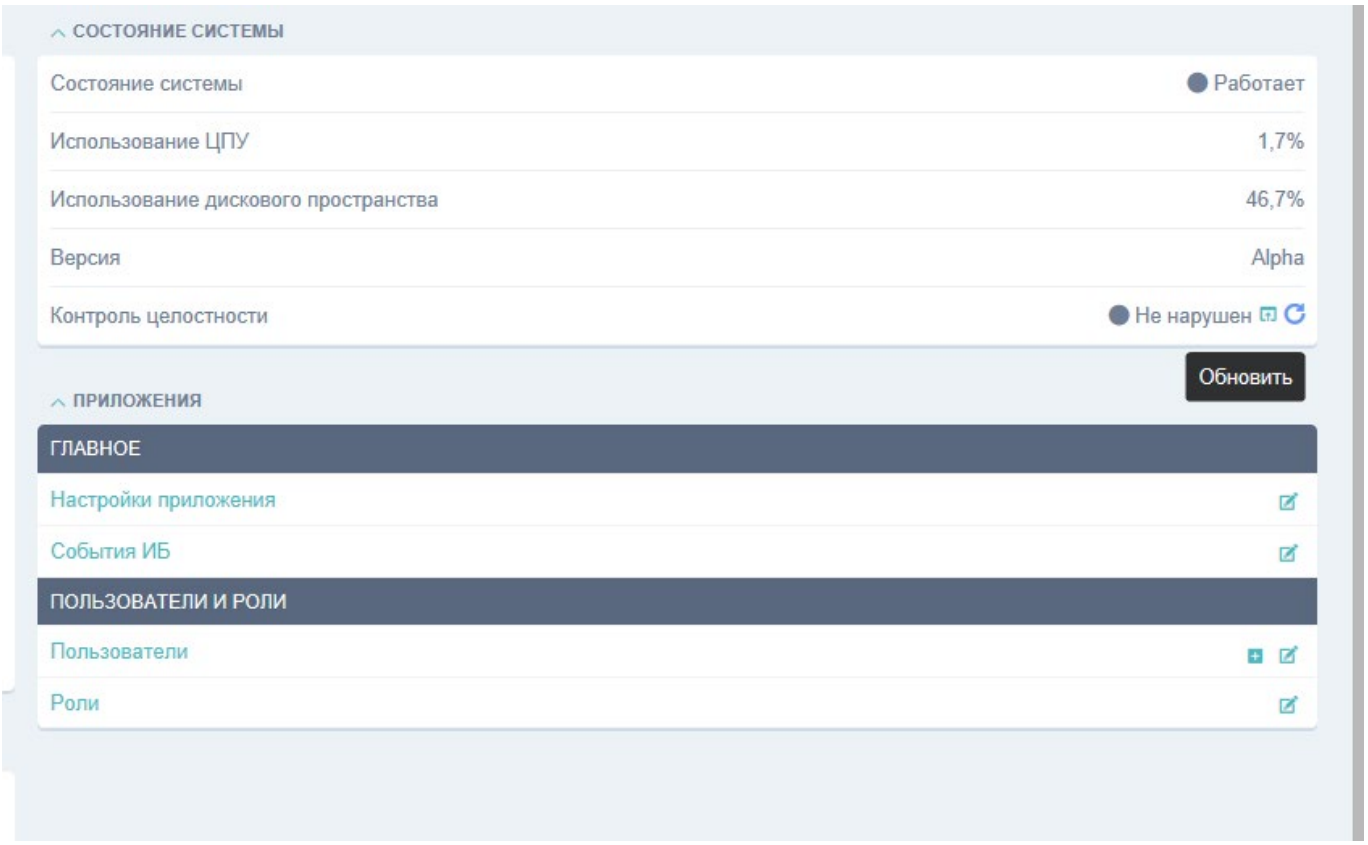

Рис. 19

Работа пользователя в программе

Для работы пользователя в программе используется графический интерфейс программы.

Пользователь осуществляет наблюдения за событиями системы обнаружения вторжений, поступающих в графический интерфейс на АРМ Администратора, подключенного по отдельному сетевому интерфейсу к серверу СОВ.

Вход в программу

Доступ к графическому интерфейсу программы осуществляется с помощью браузера посредством ввода в адресную строку IP-адреса изделия, полученного в ходе настройки изделия. После ввода в адресную строку IP-адреса изделия следует открытие страницы входа в программу (рис. 20).

Для входа в программу ввести имя и пароль пользователя.

Имя и пароль пользователя созданы администратором при настройке программы.

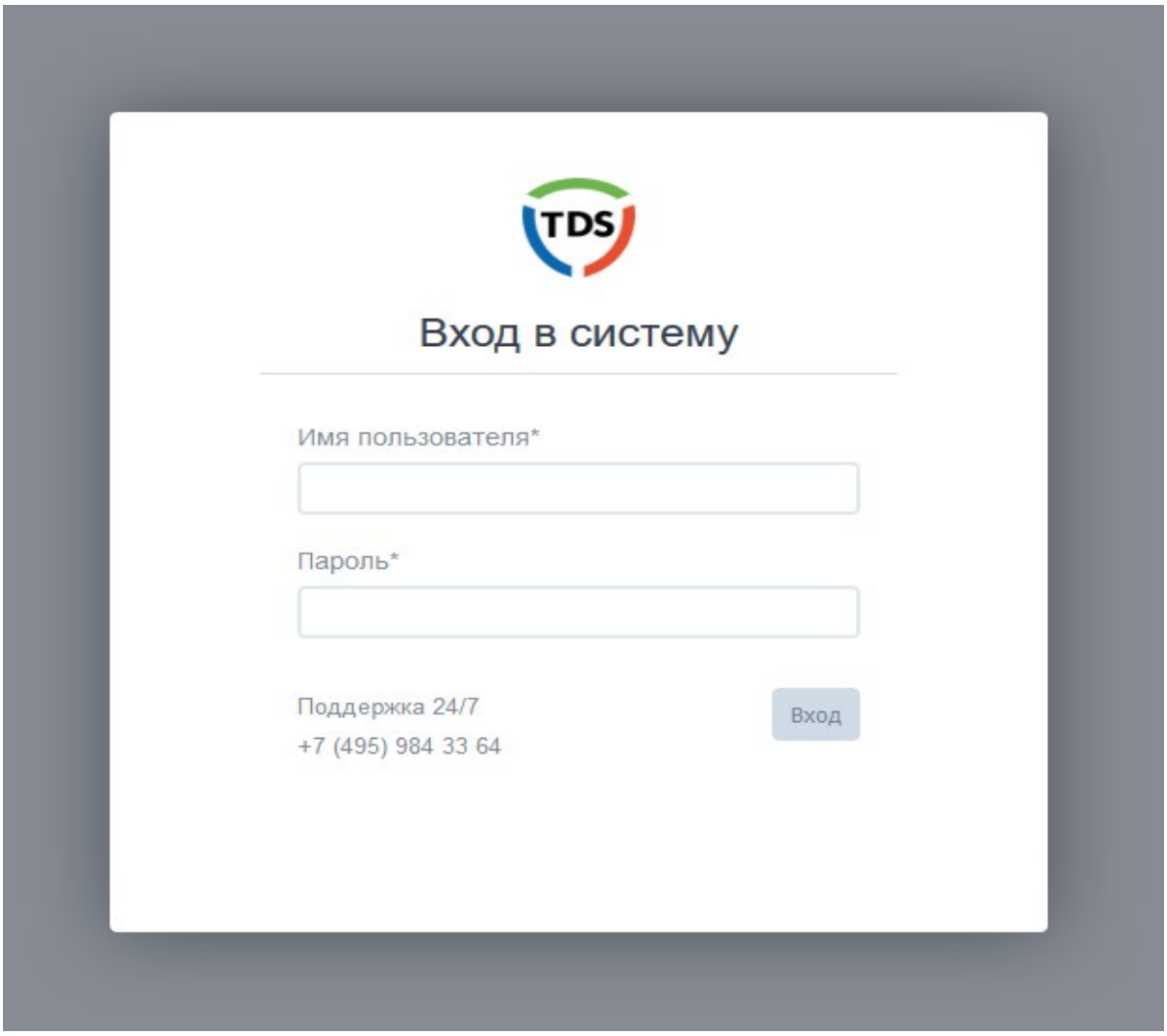

Рис. 20

Главное окно программы

После ввода имени и пароля пользователя откроется главное окно программы (рис. 21).

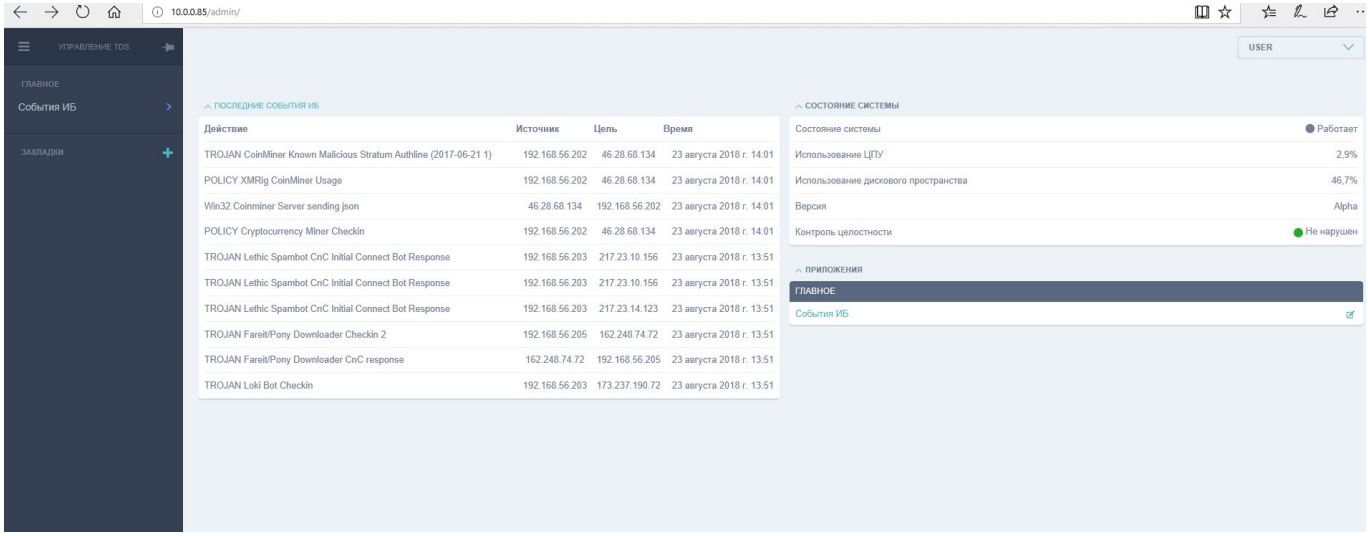

Рис. 21

В главном окне программы следует выделить следующие экранные области:

– область «Управление TDS» – служит для вывода доступных функций программы для пользователя;

– основная область вывода информации.

В основной области вывода информации можно посмотреть «Последние события ИБ» и «Состояние системы».

В окне «Состояние системы» представлена следующая информация о системе:

– Состояние системы;

– Использование ЦПУ;

– Использование дискового пространства;

– Версия;

– Контроль целостности.

Редактирование учетной записи пользователей

Пользователю программы доступна функция смены пароля. Для смены пароля необходимо в выпадающем окне с именем пользователя в правом верхнем углу главного окна программы выбрать пункт меню «Изменить пароль» (рис. 22).

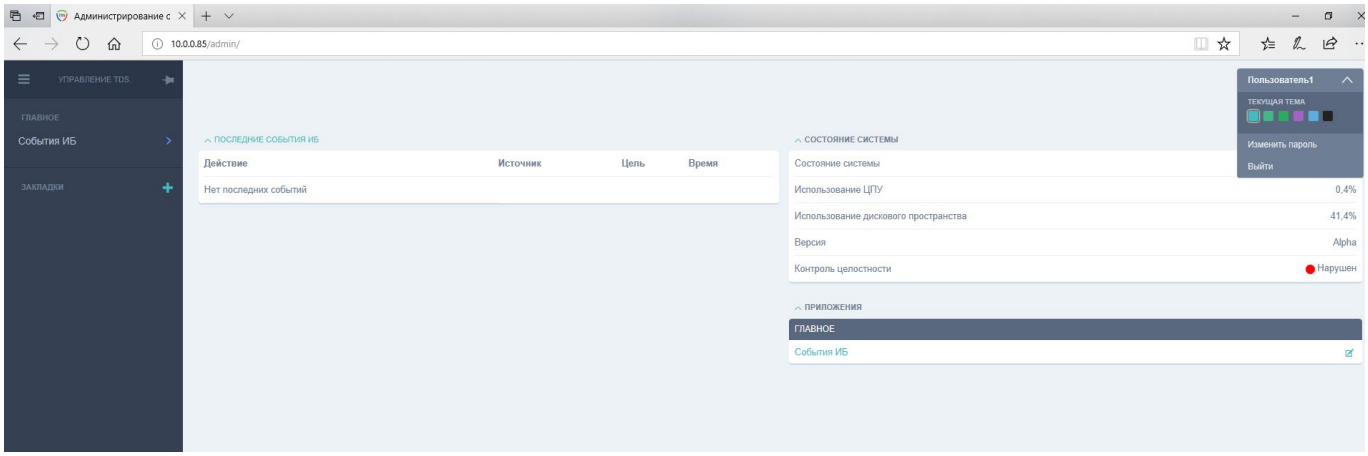

Рис. 22

Далее в появившемся окне «Изменение пароля» ввести старый пароль, а затем дважды новый пароль (рис. 23) и нажать кнопку [Изменить мой пароль].

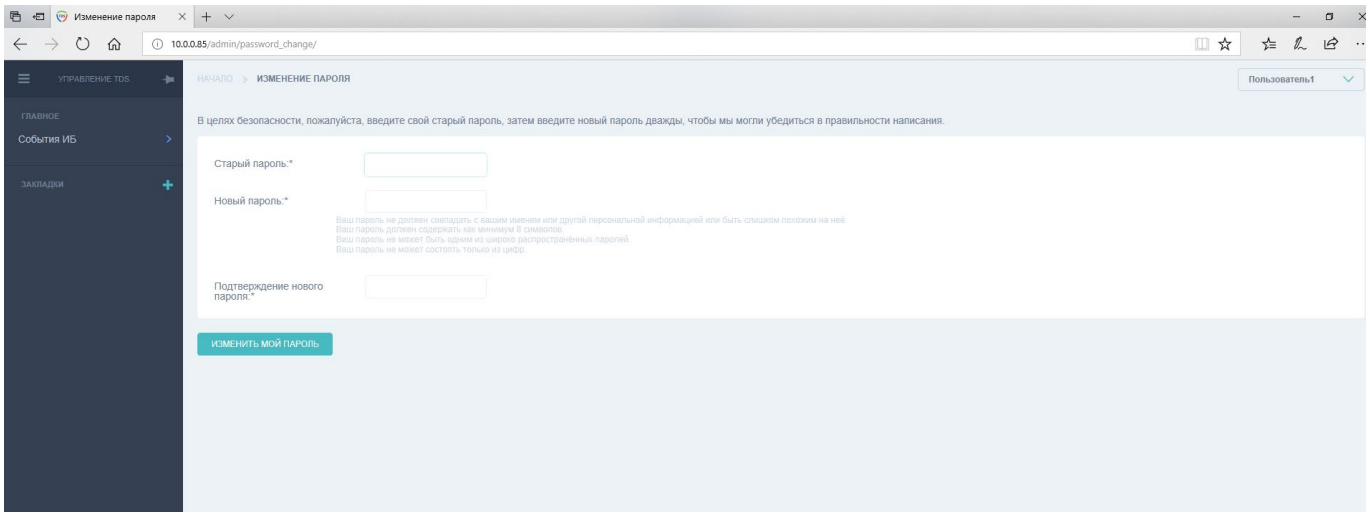

Рис. 23

В случае если пароль не соответствует политике безопасности программа выдаст предупреждение о невозможности смены пароля (рис. 24).

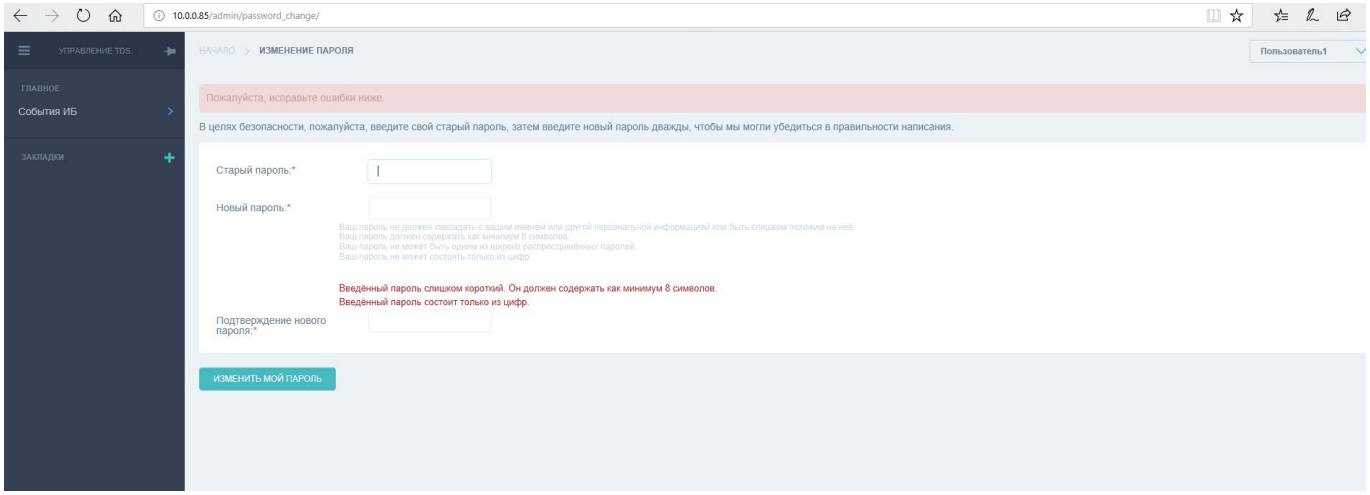

Рис. 24

Мониторинг событий

Для наблюдения за событиями системы обнаружения вторжений пользователю доступна функция «События ИБ».

Функция «События ИБ» предназначена для информирования пользователя об обнаруженных вторжениях в режиме реального времени и вывода статистической информации.

Окно программы «Последние события ИБ» позволяет просматривать следующую информацию, поступающую в программу (рис. 25):

- Действие;
- Источник;
- Цель;

– Время.

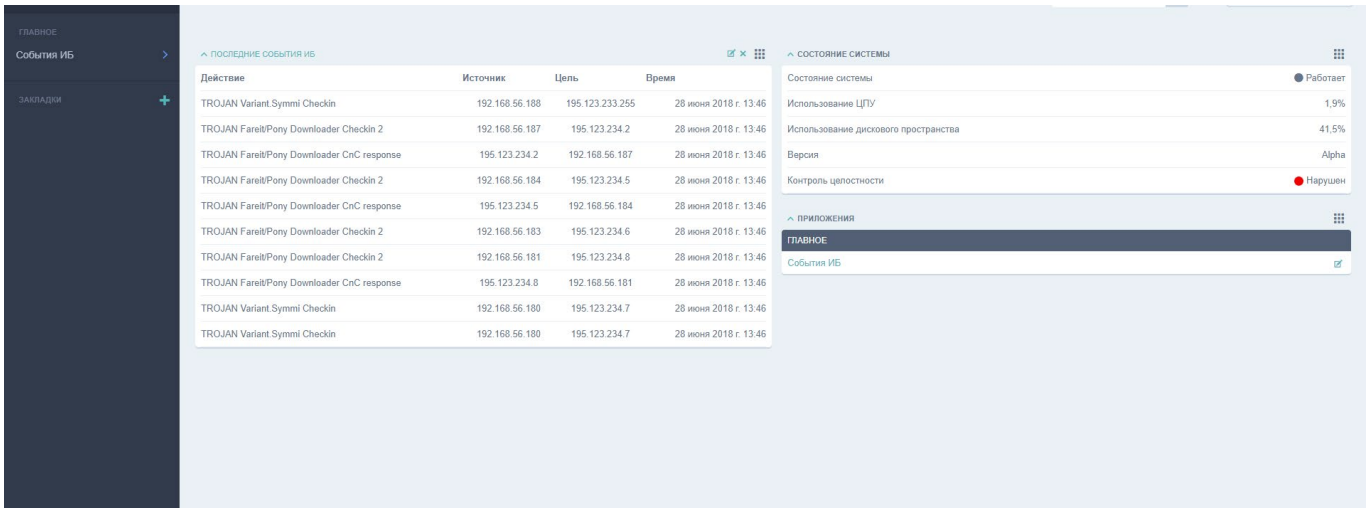

Рис. 25

Для запуска функции «События ИБ» необходимо нажать на вкладку «События ИБ» в области «Управление TDS». Откроется окно, как показано на рис. 26.

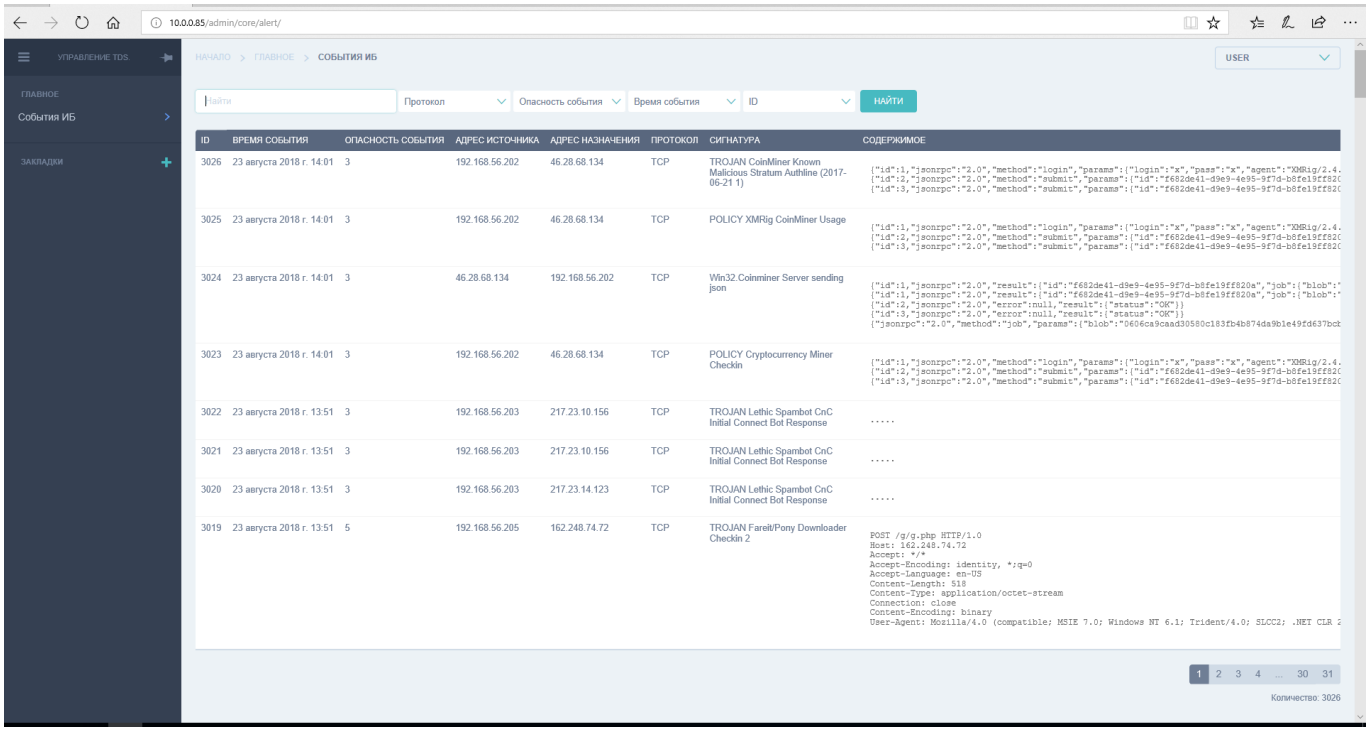

Рис. 26

Для работы пользователя доступны следующие функции:

– поиск по ключевым словам в событиях;
– фильтры:
  – по протоколу;
  – опасности события;
  – времени события;

– ID события.

Оповещения программы

Оповещение осуществляется путем обновления страницы со списком событий ИБ.

Для обновления страницы нажать на клавиатуре клавишу <F5>. Появится значок и поле с описанием как показано на рис. 27.

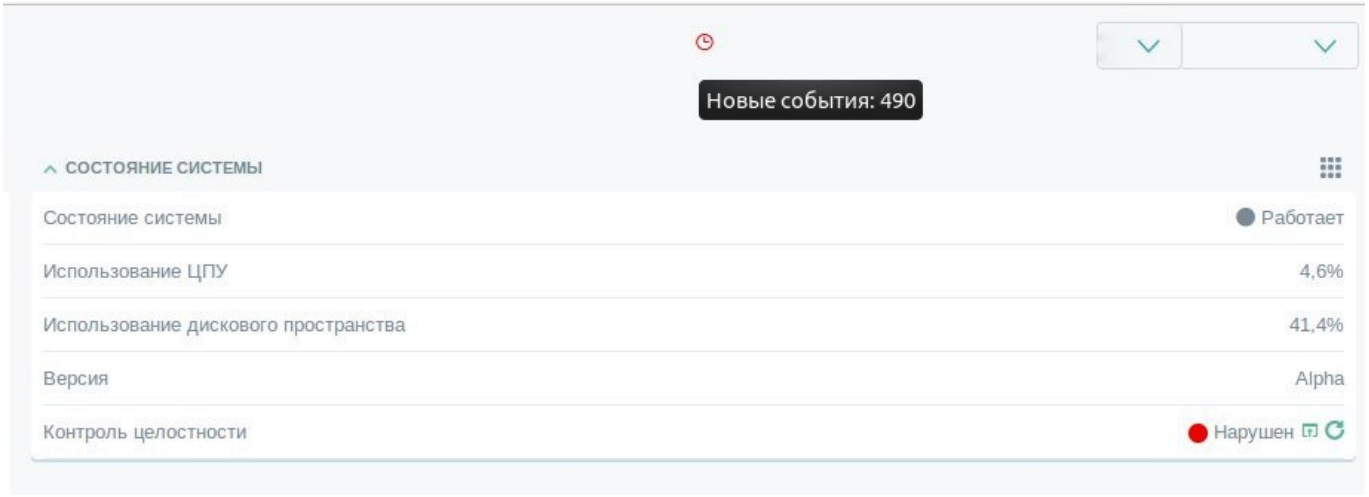

Рис. 27