R-Vision

R-Vision UEBA

Руководство пользователя

Версия 1.3

ОГЛАВЛЕНИЕ

1. О продукте 5
1.1. Как работает система 5
2. Вход в систему 7
3. Выход из системы 8
4. Просмотр уведомлений системы 9
5. Пользователи системы 10
5.1.1. Пользователи системы: добавление 10
5.1.2. Пользователи системы: изменение статуса 10
5.1.3. Пользователи системы: удаление 11
5.2. Списки 11
5.2.1. Добавление списка 12
5.2.2. Удаление списка 13
5.2.3. Восстановление списка 13
6. Программные эксперты: обучение и анализ данных 15
6.1. О программных экспертах 15
6.2. Настройка обучения системы 15
6.3. Управление экспертами 16
6.3.1. Включение и выключение эксперта 17
7. Корреляция данных: настройка простых правил 18
7.1. О простых правилах 18
7.2. Добавление правил 18
7.3. Включение и выключение простого правила 19
7.4. Удаление правил 20
7.5. Восстановление правил 20
8. Работа с оповещениями 21
8.1. Об оповещениях 21
8.2. Добавление правила оповещения 21
8.3. Просмотр оповещений 22
8.4. Управление правилами оповещения 23
8.5. Включение и выключение правила 23
8.6. Оповещение: просмотр хронологии событий 23
9. Просмотр сводных данных 25
9.1. Об отображении сводной информации 25
9.2. Добавление виджета на дашборд 25
9.3. Добавление дашборда 26
9.4. Просмотр данных на дашбордах 26
10. Просмотр объектов наблюдения 28
10.1. Об объектах наблюдения 28

10.2. Просмотр информации об объекте 28
10.3. Просмотр хронологии объекта наблюдения 29

11. Настройка системы 31
11.1. Лицензия 31
11.2. Пользователи 31

11.2.1. Добавление учетной записи 31

11.2.2. Изменение статуса учетной записи 32
11.3. Интеграция с электронной почтой 32

1. О ПРОДУКТЕ

R-Vision UEBA детектирует нарушения в состоянии систем, подозрительную активность объектов и осуществляет динамическую оценку угроз и аномалий.

Аналитические возможности R-Vision UEBA повышают эффективность работы центра управления безопасностью (SOC): в потоке подозрительных событий и инцидентов выявляют признаки начинающейся атаки и назначают приоритеты угрозам.

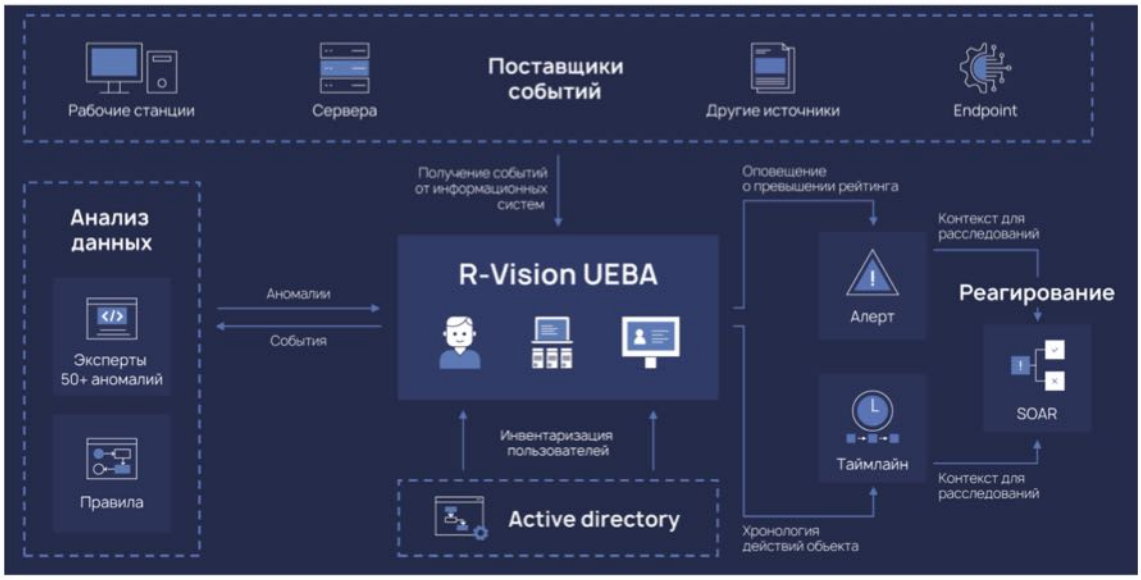
1.1. Как работает система

R-Vision UEBA непрерывно отслеживает события безопасности, анализируя данные из различных источников: систем лог-менеджмента, SIEM-систем и других. Платформа анализирует события, связанные с конкретными объектами, например, пользователями, узлами, файлами, сервисами.

Изучая поведение объектов, R-Vision UEBA формирует профили нормального поведения и фиксирует подозрительную активность при обнаружении отклонений. Система динамической оценки угроз и аномалий рассчитывает рейтинг опасности контролируемых объектов. При обнаружении подозрительной активности рейтинг (скор) объекта увеличивается, и в случае превышения допустимого уровня аналитик получит оповещение.

R-Vision UEB Аавтоматически совершенствует встроенную аналитику по выявлению аномалий. При появлении новых источников и моделей данных простые правила и программные эксперты адаптируются в автоматическом режиме и не требуют донастройки. Для анализа данных платформа использует универсальный формат, что позволяет реализовать гибкие алгоритмы детектирования отклонений.

Подробная информация о подозрительной активности объектов сохраняется в виде таймлайна – временной шкалы, на которой отмечаются аномалии, выстраивается последовательность событий и контекст. Таймлайн значительно упрощает анализ инцидентов и выявление проблем в защите для устранения.



R-Vision UEBA:

- Непрерывно контролирует и выявляет изменения в состоянии безопасности. Осуществляет раннее предупреждение об угрозах.
- Обнаруживает скрытые и неочевидные угрозы, ранее неизвестные атаки.
- Определяет критичность угроз и аномалий, фокусирует внимание аналитика на угрозах и аномалиях с высоким рейтингом опасности.
- Снижает количество инцидентов и ложных срабатываний за счет самообучающихся аналитических алгоритмов.
- Упрощает анализ инцидентов и отображает последовательность событий на таймлайне.

2. ВХОД В СИСТЕМУ

После установки и настройки веб-интерфейс платформы доступен по ссылке `http://<dns-имя сервера>`, если внесена соответствующая A-запись на DNS-сервере.

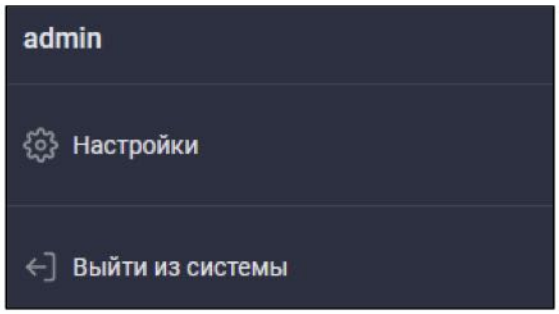
После перехода по ссылке в окне браузера отобразится окно авторизации. Для выполнения авторизации и входа в систему укажите логин и пароль учетной записи пользователя и нажмите на кнопку **Войти**.

Если вход в систему выполнен успешно, то в окне браузера отобразится стартовый раздел системы. В правом верхнем углу экрана отобразится текущая учетная запись.

3. ВЫХОД ИЗ СИСТЕМЫ

Чтобы выйти из системы:

1. Откройте меню вашей учетной записи в правом верхнем углу экрана.
2. Нажмите на кнопку **Выйти из системы** ().



Система завершит сеанс, и на экране отобразится форма ввода логина и пароля. Вы можете осуществить повторный вход в систему с помощью той же или другой учетной записи.

4. ПРОСМОТР УВЕДОМЛЕНИЙ СИСТЕМЫ

Система отображает уведомления о следующих событиях:

- оповещения системы;
- системные ошибки;
- уведомления о состоянии системы.

Просмотреть список уведомлений можно по кнопке  в верхней части экрана.

В списке отображается название, дата и время произошедшего события.

События можно удалить:

1. По одному по кнопке **Удалить** () в списке.
2. Удалить все события: по кнопке **Очистить** () над списком.

Вы можете отключить уведомления по кнопке **Не беспокоить** над списком. Уведомления будут отключены. Нажмите повторно для того, чтобы вновь активировать уведомления.

5. ПОЛЬЗОВАТЕЛИ СИСТЕМЫ

В этом разделе приведены инструкции по добавлению и редактированию пользователей в системе.

- Пользователи системы: добавление
- Пользователи системы: изменение статуса
- Пользователи системы: удаление

5.1.1. Пользователи системы: добавление

Для добавления учетной записи пользователя системы:

1. Перейдите в раздел **Настройки системы → Пользователи**.
2. Нажмите на кнопку **Добавить**. На экране отобразится окно добавления пользователя.
3. Введите логин и пароль для учетной записи пользователя.
4. Введите описание пользователя.
5. Выберите роль пользователя: администратор или пользователь.
6. Выберите статус учетной записи: включен или выключен. Статус учетной записи можно будет поменять после создания.
7. Нажмите на кнопку **Добавить пользователя**. Учетная запись отобразится в списке с выбранным статусом.

Чтобы очистить форму данных нового пользователя не сохраняя информацию, нажмите на кнопку **Отменить**. Все поля будут очищены, и вы сможете заполнить форму нового пользователя с нуля.

Чтобы закрыть окно добавления пользователя, нажмите на крестик в правом верхнем углу.

5.1.2. Пользователи системы: изменение статуса

Чтобы изменить статус учетной записи пользователя системы:

1. Перейдите в раздел **Настройки системы → Пользователи**.
2. В списке пользователей в столбце **Статус** переключите состояние учетной записи любым из двух способов:

a. Щелчком мыши на переключателе в списке:

    1. Переключатель в правом положении: учетная запись в статусе **Включен**. Учетную запись можно использовать.

    2. Переключатель в левом положении: учетная запись в статусе **Выключен**. Учетную запись нельзя использовать.

b. С помощью переключателя в свойствах учетной записи пользователя.

5.1.3. Пользователи системы: удаление

Чтобы удалить пользователя:

1. Перейдите в раздел **Настройки системы → Пользователи**.
2. В списке выберите пользователя, которого хотите удалить.
3. Удалите пользователя любым из следующих способов:

    1. Нажмите на кнопку **Удалить** () в строке пользователя. Кнопка появляется по наведению курсора мыши на строку в списке.

    2. Нажмите на кнопку с надписью **Удалить** вверху экрана.

4. Подтвердите удаление. Пользователь будет удален из системы.

Чтобы удалить нескольких пользователей:

1. Установите в списке флажки напротив пользователей, которых хотите удалить.
2. Нажмите на кнопку с надписью **Удалить** вверху экрана.
3. Подтвердите удаление. Пользователи будут удалены из системы.

5.2. Списки

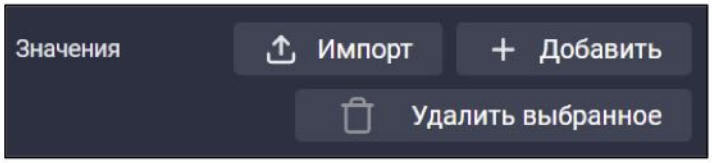
Списки — это наборы значений в системе (например, список пользователей с правами администратора, список опасных программ). Списки можно использовать для передачи значений в простых правилах и обогащении данных.

Управлять списками можно в разделе **Настройки системы → Списки**.

5.2.1. Добавление списка

Чтобы добавить список:

1. Перейдите в раздел **Настройки системы → Списки → Действующие**.
2. Нажмите на кнопку **Добавить**. В правой части экрана отобразятся параметры списка.
3. Заполните поля:
   - Имя.
   - Описание.
4. Добавьте значения в список одним из двух способов:
   a. С помощью кнопки **Добавить** в блоке операций со значениями:



   Введите значение и подтвердите ввод кнопкой . Добавленное значение появится в списке под полем ввода, где его можно отредактировать с помощью кнопки .

   b. Из файлов в форматах .csv и .xls по кнопке **Импорт**.
5. Чтобы удалить значение, воспользуйтесь одним из следующих способов:
   a. Если нужно удалить одно значение, выделите его в списке и нажмите кнопку **Удалить** ( ). Кнопка становится доступна при наведении курсора мыши на строку в списке.
   b. Если нужно удалить несколько значений, выделите их в списке и нажмите кнопку **Удалить выбранное** в блоке операций со значениями.

> Если в списке много значений, для удобства вы можете воспользоваться панелью поиска, которая находится под кнопками действий со значениями. Начните вводить

название значения, и система отфильтрует результаты по введенному фрагменту текста.

6. Нажмите на кнопку **Добавить список**. Список отобразится в разделе **Настройки системы → Списки**.

5.2.2. Удаление списка

Чтобы удалить один список с возможностью восстановления:

1. Перейдите в раздел **Настройки системы → Списки → Действующие**.
2. Выберите список, который хотите удалить.
3. Удалите список любым из следующих способов:
   a. В строке списка нажмите на кнопку **Удалить** (). Кнопка становится доступна при наведении курсора мыши на строку в списке.
   b. Нажмите на кнопку с надписью **Удалить** вверху экрана.
4. Подтвердите удаление. Список переместится в раздел **Удаленные**.

Чтобы удалить несколько списков с возможностью восстановления:

1. В разделе **Настройки системы → Списки → Действующие** установите флажки напротив списков, которые хотите удалить.
2. Нажмите на кнопку с надписью **Удалить** вверху экрана.
3. Подтвердите удаление. Списки переместятся в раздел **Удаленные**.

Если вы удалите список из раздела **Удаленные**, восстановить этот список будет уже нельзя.

5.2.3. Восстановление списка

Чтобы восстановить удаленный список:

1. Перейдите в раздел **Настройки системы → Списки → Удаленные**.
2. Выберите список.

3. Нажмите на кнопку **Восстановить** (). Кнопка становится доступна при наведении курсора мыши на строку в списке. Если нужно восстановить несколько списков, отметьте их флажками и нажмите кнопку с текстом **Восстановить** вверху экрана.

6. ПРОГРАММНЫЕ ЭКСПЕРТЫ: ОБУЧЕНИЕ И АНАЛИЗ ДАННЫХ

В этом разделе приведено описание настройки обучения программных экспертов и анализа данных.

6.1. О программных экспертах

Программные эксперты в составе системы анализируют журналы объектов наблюдения для поиска аномалий.

С помощью многоуровневой системы программных экспертов платформа постоянно контролирует:

- запуск процессов и приложений,
- запросы аутентификации,
- доступ процессов к файлам,
- подключения VPN,
- определение DGA и look-a-like доменов
- почтовый трафик и другие параметры.

Перед началом анализа данных журналов систему нужно обучить. В процессе обучения программные эксперты собирают данные о нормальном состоянии системы.

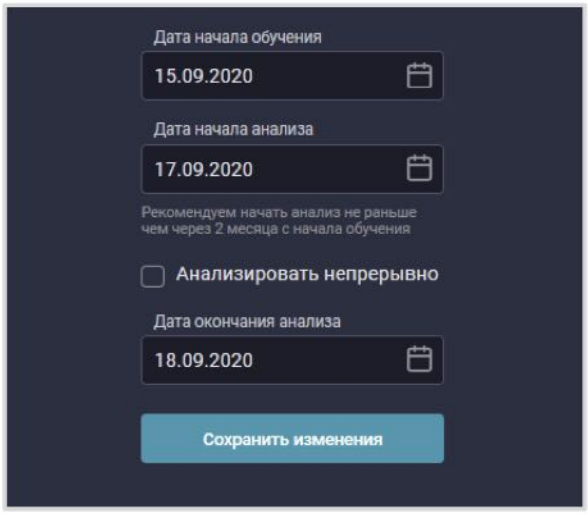
Данные о нормальном состоянии системы служат основой для поиска аномалий в режиме анализа данных. Отклонения от нормального состояния будут рассматриваться как аномалии.

Система использует обнаруженные аномалии при расчете скора объекта наблюдения. Скор рассчитывается постоянно по всем полученным индикаторам. При обнаружении подозрительной активности скор объекта увеличивается, и в случае превышения допустимого уровня аналитик получит оповещение.

6.2. Настройка обучения системы

Чтобы настроить обучение системы:

3. Перейдите в раздел **Настройки → Обучение и скоринг.**



4. В поле **Дата начала обучения** укажите дату, с которой система начинает наблюдение за объектами для обучения программных экспертов. Обнаружение аномалий при этом не проводится.
5. В поле **Дата начала анализа** укажите дату, с которой система начинает анализ данных. С этой даты система прекращает обучение и начинает анализировать данные. Чтобы не указывать срок окончания анализа данных, установите флажок **Анализировать непрерывно**.

> Рекомендуемый срок обучения - один месяц. Минимальный срок обучения для корректной работы системы - две недели.
>
> Рекомендуется повторять обучение системы раз в два месяца, но не реже, чем раз в шесть месяцев.

6. Нажмите на кнопку **Сохранить изменения**. Система начнет обучение, которое будет продолжаться до даты начала анализа. Если система перешла в режим анализа, то она будет анализировать данные до его окончания.

6.3. Управление экспертами

Просмотреть список экспертов можно в разделе **Эксперты**.

Чтобы просмотреть свойства эксперта, откройте карточку эксперта щелчком на строке эксперта. В правой части экрана отобразится информация об эксперте.

6.3.1. Включение и выключение эксперта

Слева от названия эксперта отображается переключатель состояния. Эксперт в активном состоянии анализирует данные. Неактивный эксперт не используется для анализа данных.

Чтобы переключить состояние эксперта:

1. Откройте список экспертов в разделе **Эксперты**.
2. В строке правила переключите состояние эксперта щелчком мыши на переключателе:

   a. Переключатель в правом положении: эксперт активен и используется.

   b. Переключатель в левом положении: эксперт отключен.

Неактивные эксперты в списке отображаются после активных.

7. КОРРЕЛЯЦИЯ ДАННЫХ: НАСТРОЙКА ПРОСТЫХ ПРАВИЛ

В этом разделе приведена информация о настройке и управлении простыми правилами для корреляции данных.

7.1. О простых правилах

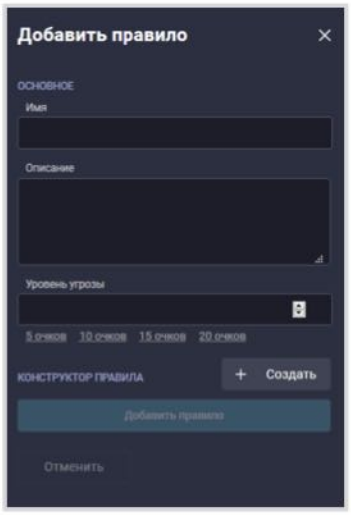
При создании простого правила пользователь задает набор критериев. События, удовлетворяющие набору критериев простого правила, помечаются индикатором правила и получают скор.

Обнаруженные события формируют скор объекта и отображаются в таймлайне.

7.2. Добавление правил

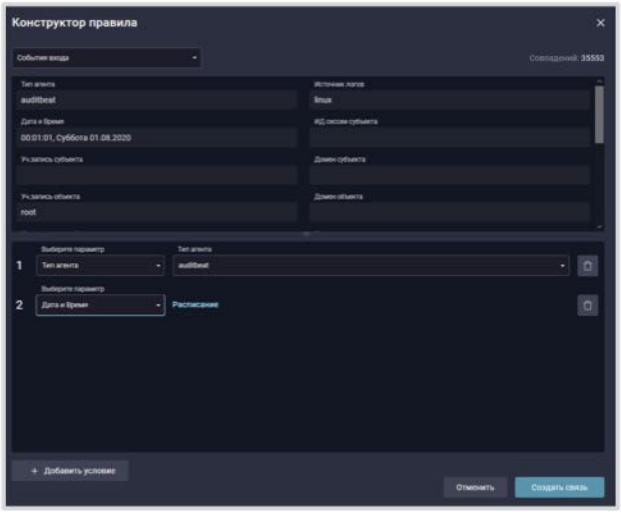
Чтобы добавить правило оповещений:

1. Перейдите в раздел **Простые правила → Список**.
2. Нажмите **Добавить**. В правой части экрана отобразится форма **Добавить правило**.



3. Заполните поля:
   a. Имя.
   b. Описание.
   c. Уровень угрозы. Уровень угрозы информирует аналитика о значении скора, который присваивает правило. Значение задается произвольно. Для быстрого ввода значения используйте набор ссылок на значения под полем.

4. В разделе **Конструктор правила** нажмите на кнопку **Создать**. На экране отобразится окно конструктора правила.



5. В появившемся окне определите критерии срабатывания правила:

c. Тип объекта, в котором система ищет аномалию. В таблице отобразится информация об объекте, которую можно использовать для настройки условий.

d. Задайте перечень условий срабатывания правила. Кнопка **Добавить условие** добавляет условия в перечень.

e. Для каждого условия выберите параметр и укажите его значение.

f. Нажмите на кнопку **Создать связь**. Информация о созданной логике отобразится в разделе Конструктор правила. Кнопка Изменить открывает окно Конструктора правила.

6. Нажмите на кнопку **Добавить правило**. Правило отобразится в списке.

7.3. Включение и выключение простого правила

Чтобы переключить состояние правила:

3. Откройте список правил в разделе **Простые правила → Список**.

4. В строке правила переключите состояние правила щелчком мыши на переключателе:

a. Переключатель в правом положении: правило активно и используется.

b. Переключатель в левом положении: правило неактивно.

Неактивные правила в списке отображаются после активных.

7.4. Удаление правил

Чтобы удалить правила:

3. Откройте список правил в разделе **Простые правила → Список**.
4. Нажмите на кнопку  для удаления правил. Правила будут удалены из списка.

Удаленные правила можно просмотреть в разделе **Простые правила→ Удаленные правила**.

7.5. Восстановление правил

Чтобы восстановить правила:

4. Откройте список удаленных правил в разделе **Простые правила → Удаленные правила**.
5. Нажмите на кнопку **Восстановить** в строке правила. Система восстановит правило и переместит его в список правил.

Восстановленное правило можно посмотреть в разделе **Простые правила → Список**.

8. РАБОТА С ОПОВЕЩЕНИЯМИ

В этом разделе приведена информация о настройке оповещения пользователей R-Vision UEBA об обнаруженных аномалиях.

8.1. Об оповещениях

Система может оповещать аналитиков об изменении скора во времени.

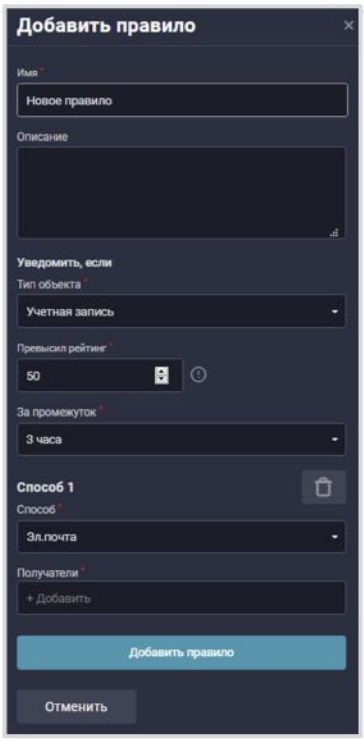
Для того, чтобы система отправляла оповещения, нужно настроить правила оповещения. Правила оповещения задают критерии отправки оповещения: при превышении заданного значения скора в течение заданного периода времени система отправляет оповещение.

Система сохраняет данные об оповещении, отправленном при срабатывании правила. Для расследования аномалии в системе можно просмотреть хронологию событий, связанных с оповещением.

8.2. Добавление правила оповещения

Чтобы добавить правило оповещений:

7. Перейдите в раздел **Оповещения → Правила оповещений**.
8. Нажмите **Добавить**. В правой части экрана отобразится форма **Добавить правило**.



9. Заполните поля:
   c. Название.
   d. Описание.
10. В разделе **Уведомить, если** укажите критерии отправки уведомления:
    a. Тип объекта, для которого определяется скор.
    b. В поле **Превысил рейтинг** укажите минимальное значение скоринга для отправки оповещений с низким уровнем угрозы. Значение определяет уровень угрозы оповещений:
       i. При превышении этого значения на 50% система присваивает оповещению средний уровень угрозы.
       ii. При превышении этого значения на 100% система присваивает оповещению высокий уровень угрозы.
    c. Укажите промежуток времени для отслеживания изменений скора.
11. Укажите способы отправки:
    a. Выберите способ отправки оповещений.
    b. Укажите получателей.
12. Нажмите на кнопку **Добавить правило**. Правило отобразится в списке.

8.3. Просмотр оповещений

Список отправленных оповещений отображается в разделе **Оповещения → Оповещения**.

Оповещения попадают в список при срабатывании правила оповещения.

Чтобы просмотреть информацию об оповещении:

5. Перейдите в раздел **Оповещения → Оповещения**.
6. В списке выберите оповещение. В правой части экрана отобразится информация об оповещении:
   c. Сработавшее правило.
   d. Информация об объекте наблюдения.

e. Статистика аномалий.

Кнопка **Расследовать** открывает хронологию событий, с которыми связано оповещение.

8.4. Управление правилами оповещения

Параметры правила оповещения можно редактировать по кнопке  в строке правила. Кнопка  удаляет правило. Удаленные правила можно просмотреть и восстановить в разделе **Оповещения → Удаленные правила**.

8.5. Включение и выключение правила

Чтобы переключить состояние правила:

4. Откройте список правил в разделе **Оповещения → Правила оповещения**.
5. В строке правила переключите состояние правила щелчком мыши на переключателе:

a. Переключатель в правом положении: правило активно и используется для отправки оповещений.

b. Переключатель в левом положении: правило неактивно. Оповещения не отправляются.

Неактивные правила в списке отображаются после активных.

Если правило выключено, то индикаторы не генерируются. При повторном включении правила можно провести ретроспективный анализ.

8.6. Оповещение: просмотр хронологии событий

Чтобы просмотреть хронологию событий, связанных с оповещением:

1. Перейдите в раздел **Оповещения → Оповещения**.
2. В списке выберите оповещение. В правой части экрана отобразится информация об оповещении.

3. Нажмите на кнопку **Расследовать**. Система откроет хронологию событий, с которыми связано оповещение.

9. ПРОСМОТР СВОДНЫХ ДАННЫХ

В этом разделе приведено описание работы со сводными данными в системе.

9.1. Об отображении сводной информации

Дашборд отображает сводные данные о работе системы. С помощью виджетов на дашборде отображаются показатели работы системы, например, список основных аномальные учетные записи, статистика событий и другое.

Количество дашбордов и набор виджетов на дашборде можно настроить. Каждый пользователь видит только свои дашборды.

Количество дашбордов и виджетов не ограничено.

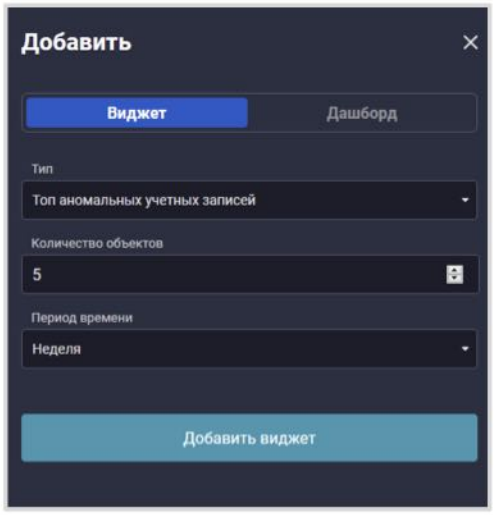
Данные обновляются автоматически.

9.2. Добавление виджета на дашборд

Виджеты отображают на дашборде информацию о показателях системы.

Чтобы добавить виджет:

1. Перейдите в раздел **Дашборд**.
2. Откройте дашборд, на который вы хотите добавить виджет. Вы можете создавать новые дашборды.
3. Нажмите на кнопку **Добавить**.
4. В правой части экрана выберите опцию **Виджет**.



5. Выберите тип виджета.

6. Укажите параметры отображаемой информации. Набор параметров зависит от выбранной категории виджета.
7. Нажмите на кнопку **Добавить виджет**. Виджет отобразится на дашборде.

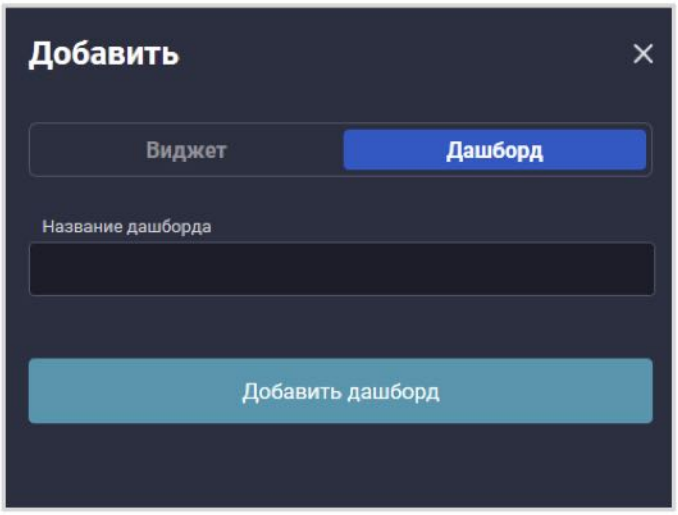
Удалить виджет можно в меню **Действия** ( ) виджета.

9.3. Добавление дашборда

Вы можете добавить несколько дашбордов для размещения виджетов.

Чтобы добавить дашборд:

1. Перейдите в раздел **Дашборды**.
2. Нажмите на кнопку **Добавить**.
3. В правой части экрана выберите опцию **Дашборд**.



4. Укажите название дашборда.
5. Нажмите на кнопку **Добавить**. На экране отобразится пустой дашборд. Для отображения информации добавьте виджеты на дашборд.

9.4. Просмотр данных на дашбордах

Чтобы просмотреть сводные данные:

1. Перейдите в раздел **Дашборд**.
2. По нажатию на название дашборда в верхней части экрана откройте список дашбордов.

3. В списке выберите дашборд для просмотра. На экране отобразится выбранный дашборд с набором виджетов.

Виджеты можно добавлять на дашборд и удалять.

Для просмотра подробной информации наведите курсор мыши на сегмент графика.

Изменить размер виджета можно, потянув за нижний правый угол.

Переместить виджет на дашборде можно перетаскиванием мышью за заголовок виджета.

10. ПРОСМОТР ОБЪЕКТОВ НАБЛЮДЕНИЯ

В этом разделе приведена инструкция по просмотру данных об объектах наблюдения.

10.1. Об объектах наблюдения

Объекты наблюдения - это объекты инфраструктуры организации (например, учетные записи пользователей, оборудование в сети организации), данные по которым отслеживает система R-Vision UEBA. Система получает данные по объектам наблюдения и связанным с ними событиям из журналов SIEM систем и Microsoft Active Directory.

Система использует простые правила и программные эксперты для обнаружения аномалий. Связанные аномалии и события сохраняются в виде таймлайна объекта. На таймлайне выстраивается последовательность событий и контекст.

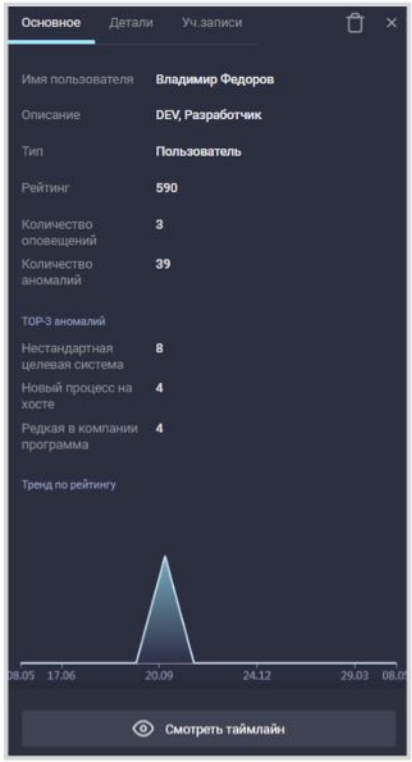
Обнаруженные аномалии повышают оценку риска объекта (скор). Система может оповещать аналитиков об изменении скора объекта и отображать информацию об изменении скора на дашборде.

10.2. Просмотр информации об объекте

Чтобы просмотреть информацию об объекте наблюдения:

1. Перейдите в раздел **Объекта наблюдения**.
2. Выберите вкладку, соответствующую типу объекта: **Пользователи**, **Учетные записи** или **Оборудование**. Для объектов **Пользователи** выберите тип: **Синхронизированные** или **Созданные**. На экране отобразится список объектов наблюдения.
3. Выберите объект. В правой части экрана отобразится краткая информация об объекте.

Кнопка **Смотреть таймлайн** отображает хронологию объекта наблюдения. Для объектов **Пользователи** в свойствах объекта отображаются вкладки с подробной информацией. Пользователей, созданных вручную, можно редактировать.



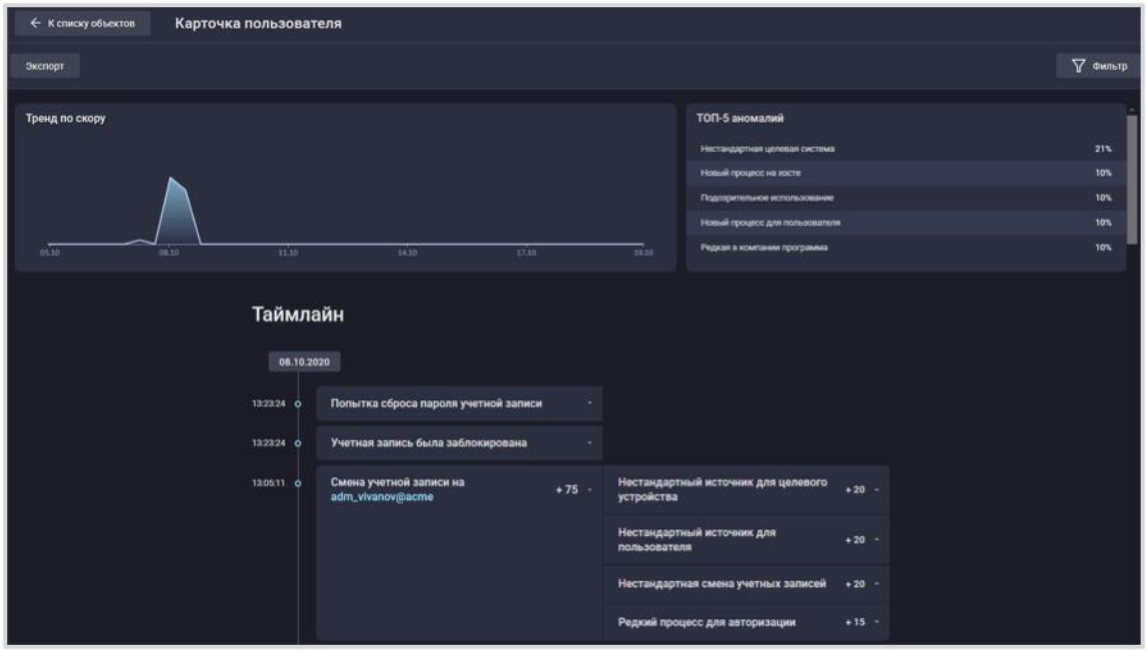
10.3. Просмотр хронологии объекта наблюдения

Чтобы просмотреть хронологию объекта наблюдения:

1. Перейдите в раздел **Объекта наблюдения**.
2. Выберите вкладку, соответствующую типу объекта: **Пользователи**, **Учетные записи** или **Оборудование**. На экране отобразится список объектов наблюдения.
3. Выберите объект. В правой части экрана отобразится краткая информация об объекте.
4. Нажмите на кнопку **Смотреть полную информацию**. На экране отобразится таймлайн объекта наблюдения.

На таймлайне отображаются блоки с информацией о событиях, связанных с объектом наблюдения. Для блока указана метка времени.

Стрелка ( ) справа от заголовка блока означает, что в блоке доступна дополнительная информация о событии. Для просмотра информации щелкните на стрелку. Информация сворачивается повторным щелчком на стрелке.


К списку объектов
Карточка пользователя
Экспорт
Фильтр
Тренд по скору
05.10
08.10
11.10
14.10
17.10
19.10
ТОП-5 аномалий
Нестандартная целевая система 21%
Новый процесс на хосте 10%
Подозрительное использование 10%
Новый процесс для пользователя 10%
Редкая в компании программа 10%
Таймлайн
08.10.2020
13:23:24
Попытка сброса пароля учетной записи
13:23:24
Учетная запись была заблокирована
13:05:11
Смена учетной записи на adm_vivanov@acme
+ 75
Нестандартный источник для целевого устройства + 20
Нестандартный источник для пользователя + 20
Нестандартная смена учетных записей + 20
Редкий процесс для авторизации + 15

11. НАСТРОЙКА СИСТЕМЫ

В этом разделе приведено описание параметров платформы и даны рекомендации по настройке.

11.1. Лицензия

Лицензия предоставляет доступ к функциям Системы.

Управлять лицензией можно в разделе **Настройки → Лицензия**. Лицензия выдается на идентификатор, созданной при установке R-Vision UEBA. Идентификатор отображается в разделе **Настройки → Лицензия** Только одна лицензия может быть активна в системе.

Как установить лицензию:

1. Перейдите в раздел **Настройки → Лицензия**. В списке отобразятся активные лицензии.
2. Нажмите на кнопку **Изменить лицензию**. На экране отобразится окно загрузки лицензии.
3. Нажмите на кнопку **Загрузить ключ** и выберите файл ключа.
4. Примените выбранный ключ по кнопке **Применить ключ**. Лицензия будет загружена в систему.

11.2. Пользователи

В этом разделе приведены инструкции по добавлению пользователей в систему.

11.2.1. Добавление учетной записи

Для добавления учетной записи пользователя:

1. Перейдите в раздел **Настройки → Пользователи**.
2. Нажмите на кнопку **Добавить пользователя**. На экране отобразится окно свойств пользователя.
3. Введите логин и пароль для учетной записи пользователя.
4. Выберите роль пользователя: администратор или пользователь.
5. Выберите статус учетной записи: включен или выключен. Статус учетной записи можно будет поменять после создания.
6. Нажмите на кнопку **Добавить пользователя**. Учетная запись отобразится в списке с выбранным статусом.

11.2.2. Изменение статуса учетной записи

Чтобы изменить статус учетной записи пользователя:

1. Перейдите в раздел **Настройки → Пользователи**.
2. В списке пользователей в столбце **Статус** переключите состояние учетной записи любым из двух способов:

a. Щелчком мыши на переключателе в списке:

i. Переключатель в правом положении: учетная запись в статусе **Включен**. Учетную запись можно использовать.

ii. Переключатель в левом положении: учетная запись в статусе **Выключен**. Учетную запись нельзя использовать.

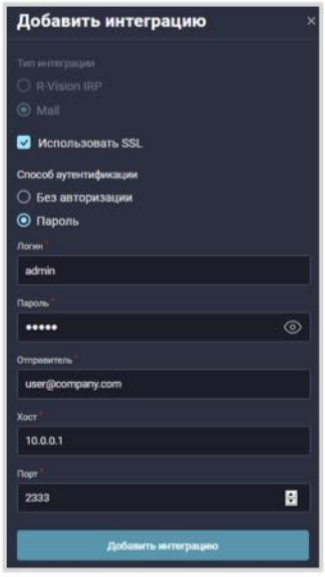
b. С помощью переключателя в свойствах учетной записи пользователя.

11.3. Интеграция с электронной почтой

Вы можете настроить отправку оповещений об обнаруженных аномалиях по электронной почте.

Чтобы настроить интеграцию с электронной почтой:

1. Перейдите в раздел **Настройки → Интеграции**.
2. Нажмите на кнопку **Добавить**. Вы можете добавить только одну интеграцию с почтовой системой. В правой части экрана отобразится карточка интеграции.



3. Установите флажок **Использовать SSL** для подключения по протоколу SSL.
4. Выберите способ авторизации: по паролю или без авторизации.
5. Заполните поля:
   a. Логин.
   b. Пароль.
   c. E-mail адрес отправителя.
   d. Хост.
   e. Порт.
6. Нажмите на кнопку **Добавить интеграцию**. Интеграция отобразится в списке.