InfoWatch Data Access Tracker 1.0

Release Notes

Бизнес-центр «Верейская плаза III»
121357, Москва, ул. Верейская, д. 29, стр. 134

+7 495 22 900 22, +7 499 37 251 74
sales@infowatch.ru

www.infowatch.ru

Улучшенный анализ доступа и новый механизм выявления аномалий в актуальном релизе системы аудита и мониторинга InfoWatch Data Access Tracker 1.0.

В InfoWatch Data Access Tracker 1.0 (далее IW DAT) расширена функциональность в части выявления аномальной активности пользователей и анализа доступа к корпоративным ресурсам:

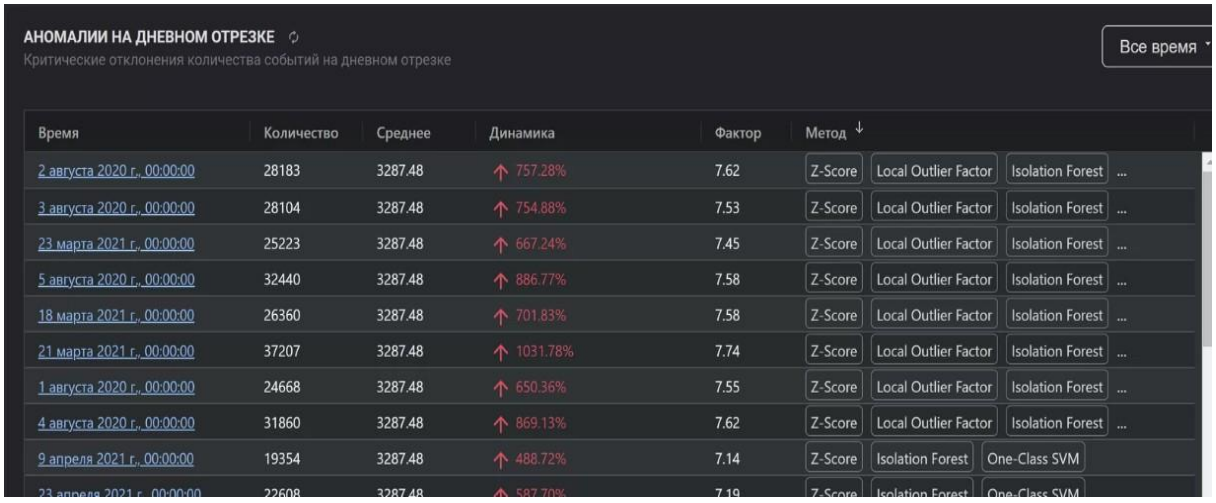
- новый механизм аномалий, который отображает критические отклонения количества событий на дневном отрезке;
- индекс атипичного поведения и параметров пользователей;
- карта параметров и поведения пользователей;
- улучшен анализ доступа пользователей к ресурсам компании.

Список изменений:

- **Новый механизм аномалий**
  К аномальному поведению можно отнести подключение к сети в нерабочее время, попытки подключения к ресурсам, к которым пользователь не допущен по должностным обязанностям, а также массовое скачивание, удаление или изменение файлов.

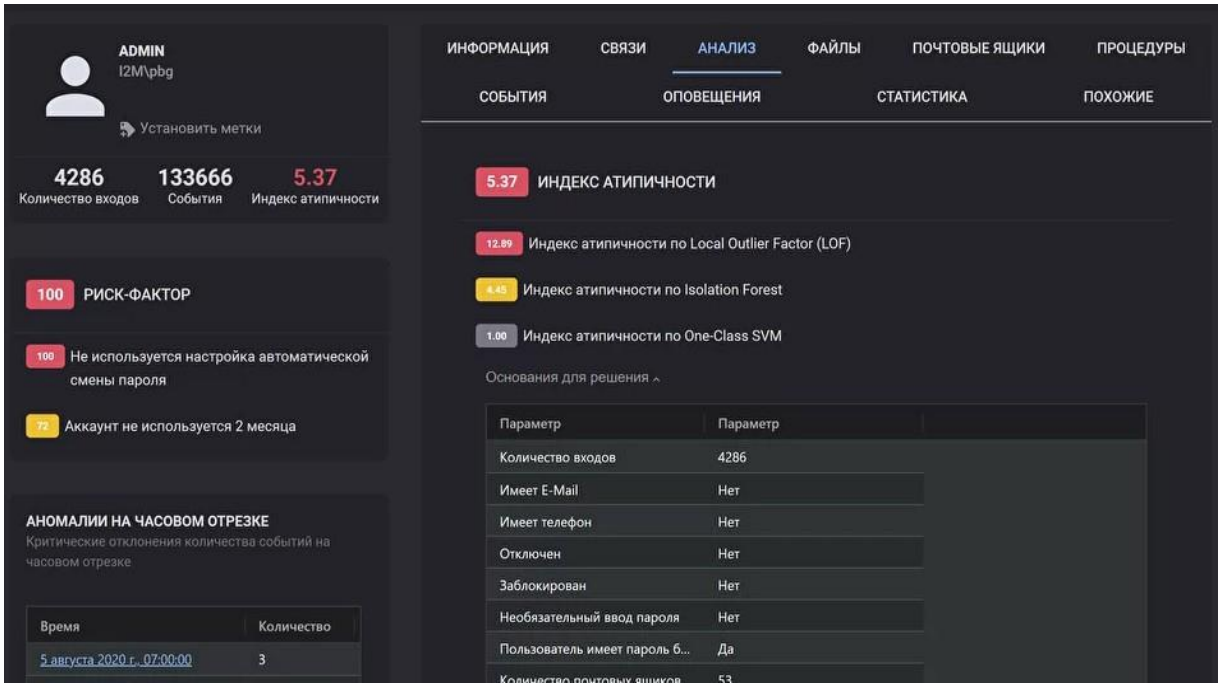
  Выявление отклонений от нормы поведения пользователя может являться поводом для дальнейшего расследования и фиксируется в разделе Аномалии.

  Для отображения динамики аномальных активностей в Системе используется таблица критических отклонений количества событий на дневном отрезке.



Аномалии на дневном отрезке

- **Индекс атипичности**
  IW DAT контролирует обращения пользователей к устройствам, файлам и почтовым ящикам. На основе полученных данных при помощи алгоритмов выявления аномалий система выстраивает индекс атипичности для каждого пользователя. Это позволяет своевременно выявить подозрительную активность и вызвать оперативную реакцию администратора.



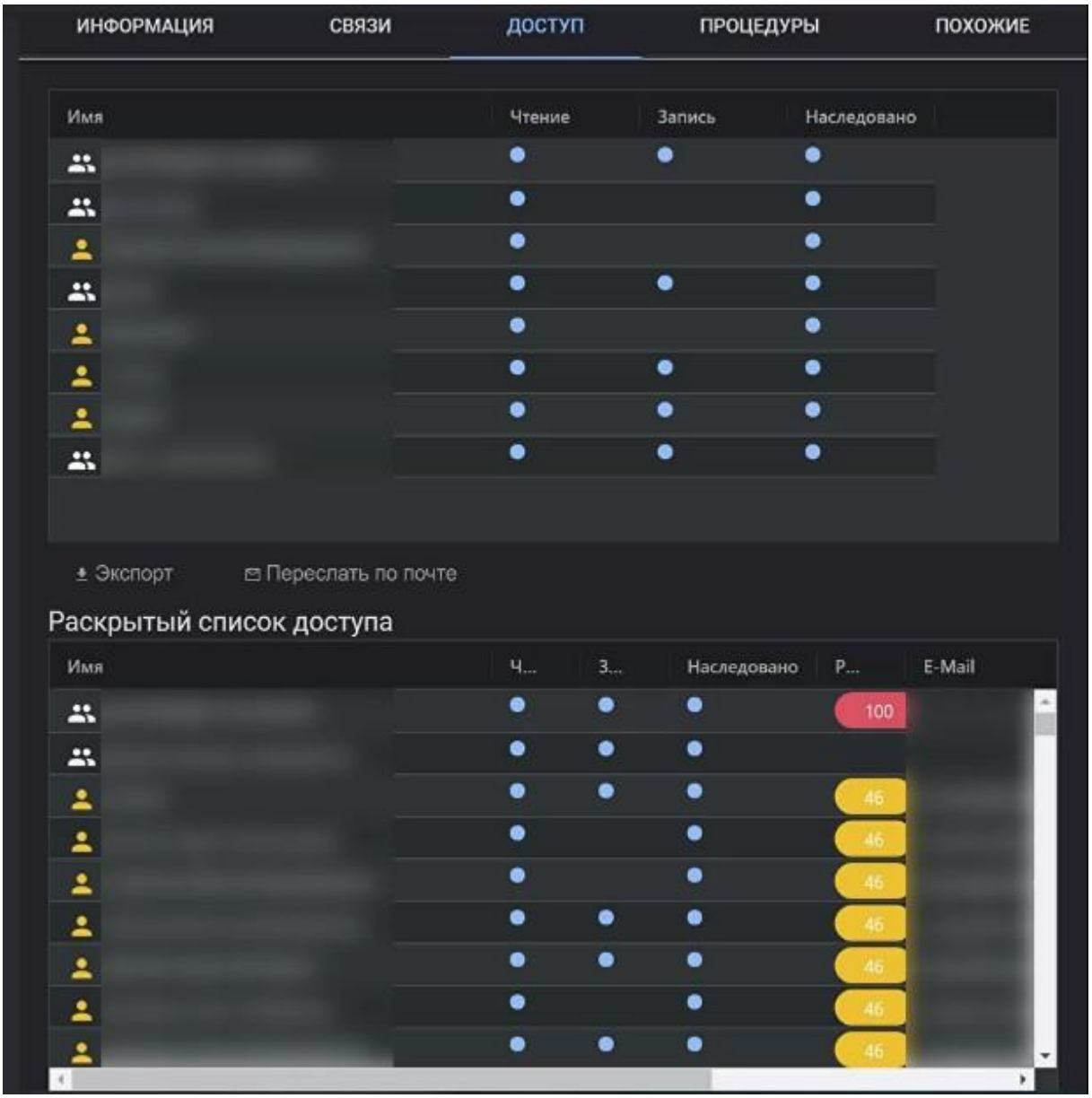
Индекс атипичности действий пользователя

- **Карта пользователей**

  В Системе появилась карта параметров и поведения пользователей, которая отображает уровень атипичной активности. Оператор может обратить внимание на пользователей с высокой степенью атипичности и принять соответствующие меры — инициировать смену пароля для пользователя, ограничить доступ к определенным ресурсам, заблокировать пользователя и так далее.

Карта параметров и поведения пользователей

- **Анализ доступа**
  В IW DAT улучшен анализ доступа к определенному ресурсу — файлу или папке. Детализированный список с настраиваемыми фильтрами, который отображает уровни доступа к конкретному файлу, наследование прав, e-mail адреса пользователей, для которых открыт доступ и риск-фактор, можно экспортировать для передачи исполнителю или отправить по e-mail прямо из консоли.



Детализация списка доступа