

INFOWATCH

InfoWatch Vision 2.0.0. User Guide

23/05/2020

© JSC “InfoWatch”

Tel/Fax +7 (495) 229-00-22

http://www.infowatch.com

Table of Contents

1 Who Should Read this Guide 4

2 Set of Documents 5

3 Technical Support 6

4 Vision Interface 7

4.1 Single filter 8

4.2 Statistics section 11

4.2.1 Statistics widgets 12

4.3 Events section 15

4.4 Connection graph section 16

4.4.1 General information about graph 17

4.4.2 Graph construction principals 20

4.5 Dossier section 24

4.5.1 Person's dossier review 25

4.5.2 Dossier widgets 26

4.5.3 Adding person's contacts 26

4.5.4 Dossiers merging 27

4.5.5 Dossier creation, editing and deletion 27

4.5.6 Changing person's manager 28

4.5.7 Person's connection graph 28

4.5.8 Commenting person's dossier 28

4.5.9 Adding file to dossier 29

5 Security officer operational scenario cases 30

5.1 Daily communications analysis for specified employees 30

5.2 Employee activity analysis 30

5.3 Detecting leakage channel 32

5.4 Specific employee communications analysis 33

5.5 Analyzing company's business processes 35

5.6 Fast search of anomalous employees conduct 37

5.7 Collecting data to dossier 40

This guide is designed to advise on InfoWatch Vision 2.0.0 System operation and effective implementation of tasks applying this software, which is intended to visualize incidents investigations in accordance with data extracted from InfoWatch Traffic Monitor.

1 Who Should Read this Guide

Information in this guide is intended for users who manage the System (perform the System configuration, analyze information objects, etc.).

The Guide is intended for users with basic knowledge of Microsoft Windows.

2 Set of Documents

InfoWatch Vision 2.0.0 documentation package includes the following:

- "InfoWatch Vision. Installation Guide". The document describes how to install, configure, update and uninstall InfoWatch Vision.
- "InfoWatch Vision. Administration Guide". The document contains information on how to configure and prepare the System for proper operation.
- "InfoWatch Vision. User Guide". The document describes the working procedures and tasks facilitating by InfoWatch Vision.

Related documents on InfoWatch Traffic Monitor include as follows:

- "InfoWatchTraffic Monitor. Installation Guide". The document describes how to install, configure, update, and uninstall the InfoWatch Traffic Monitor.
- "InfoWatch Traffic Monitor. Administration Guide". Contains information on System administration (database, server-end).
- "InfoWatch Traffic Monitor. User Guide". The document describes operation with InfoWatch Traffic Monitor: configuration setting, data export/import, creating policies for objects processing.
- "InfoWatch Traffic Monitor. Configuration files guide". The document describes the frequently used configuration files.

3 Technical Support

If you cannot resolve issues which arise when using the System or have questions regarding the use of the System, you can contact the Technical Support Service:

- If you purchased the product from an InfoWatch partner, contact the Technical Support Service of this partner company.
- If you purchased the product directly from InfoWatch, you can contact our Technical Support Service at support@infowatch.com.

Technical Support Service is available to assist you Mon-Fri, 7 AM – 9 PM (Moscow time, GMT+3), except weekends and public holidays in Russian Federation.

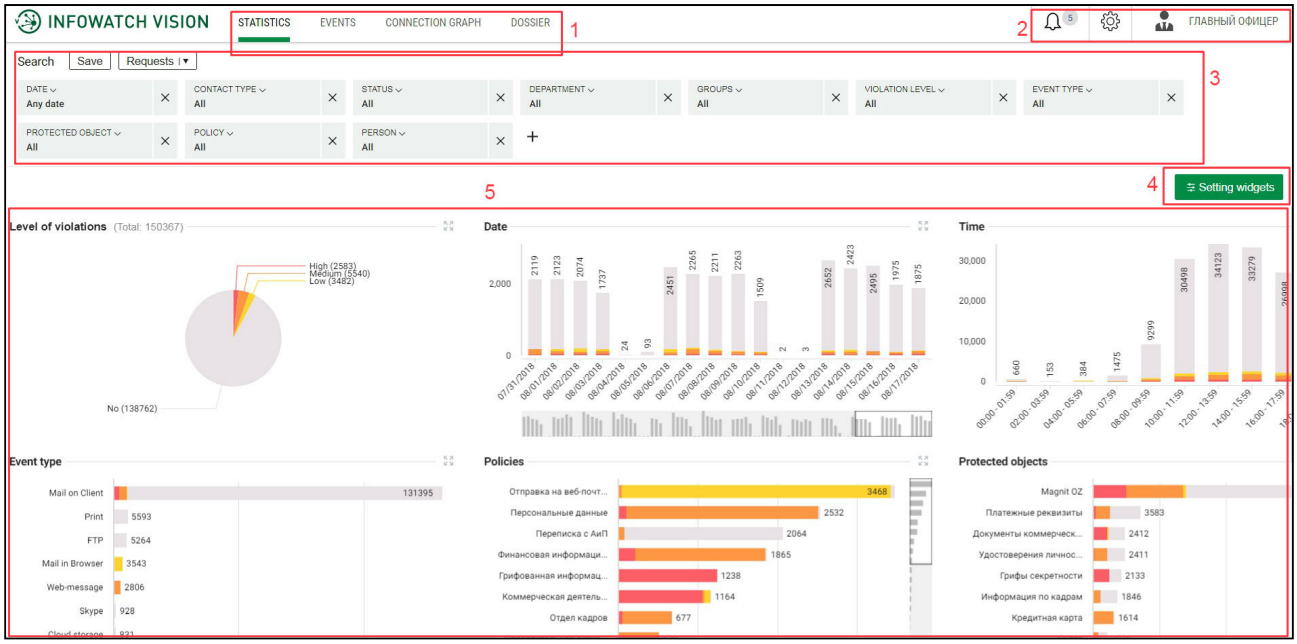
You can also visit online support at our website at: http://infowatch.com/support.

Before contacting the Technical Support Service, please refer to the Knowledge Base at our web-site: https://kb.infowatch.com/. The knowledge base may already contain the answer to your question or a description of the problem you are having.



4 Vision Interface

InfoWatch Vision interface windows contain general elements (1-3) as well as the number of specific elements (4,5).



Window elements:

Number on the scheme above	Window element	Element function
1	Navigation panel	Displaying Vision sections. When a section is selected, navigation to this section is performed.
2	Vision settings and user menu	Displaying user menu. Clicking on it a list is opened where you can take the following actions: • edit your account; • change password in your user account; • change interface language; • exit.
3	Filtration panel (Single filter)	Displaying filters you have applied. User may edit created filters as well ass add the new ones.
4	Workspace settings panel	Displaying options available for user in this section.
5	Workspace	Displaying elements of selected System section and working with them.

Vision operations are held in subject sections as per below:

Section	Description
Statistics	Section contains statistical data of violations/violators in accordance with specified filters.

Events	Section contains list of events in accordance with specified filters.
Connection graph	Section used for events visualization via connection graph.
Dossier	Section contains directory with company personnel, as well as external contacts.

4.1 Single filter

Single filter is a universal tool used in all System sections. The following functions are available for Security officer when using a single filter:

- analyzing all communications of a single person within the specific reporting period;
- saving various sets of filters to get specific reports as soon as possible;
- excluding some events from analysis to hide the information which is out of scope;
- filtering information within the connection graph to facilitate communications analysis.

To set up a filter it is enough specifying one attribute and any value. Filter is available in all System sections: **Dossier**, **Events**, **Statistics**, **Connection graph** - and it can be configured in accordance with the following attributes:

Attribute name	Attribute description and possible values
Date	The date when event happened. Specify the period of time when the data you are interested in is available. • Last 7 days; • Last 30 days; • Last 90 days; • This month; • Last month; • Custom period (you may specify the begining and the end of a period as well as a list of custom dates).
Hours	Specify the time when event happened.
Violation level	Select a violation level (comply with similar in Traffic Monitor): • High • Medium • Low • No

Event type	Event type sampling. Select the event type in Traffic Monitor: • WhatsApp; • Yahoo!; • Clipboard; • vk; • Keyboard input; • Webmail; • Crawler; • Cloud storage; • Print • Mail on client • Network resource • Social network • Removable device • Terminal session • Photography
Protected object	Select from the list of protected objects created in Traffic Monitor.
Policies	Select from the list of policies created in Traffic Monitor.
Verdict	Select verdicts you are interested in from Traffic Monitor list: *Denied, Allowed, Quarantined.*
Violations	Specify the type of search: search events with or without violations.
File name	Select the files from downloaded enclosed files in Traffic Monitor events.
Fyle type	Select the types of enclosed files in Traffic Monitor events.
Source	Select a source from the list of successfully completed integrations which data should be added into sampling: *Traffic Monitor* or *LDAP*.
Integration	Select an integration from the list of suiccessfully completed.
Contacts	Sorting of identified and unidentified contacts.
Contact type	Specify the type of search: known person's contacts in the System or person's external contacts.
Person*	Specify employee's name from the list or enter it in the search line.
Groups*	AD and Traffic Monitor groups sampling. Specify the groups within the company's hierarchical structure, which are synchronized from Traffic Monitor and Active Directory.
Title*	Specify all the company's job titles synchronized from Traffic Monitor or AD you are interested in.

Department *	Specify all the company's departments synchronized from Traffic Monitor or AD you are interested in.
Status*	Specify all the employees statuses synchronized from Traffic Monitor or AD you are interested in.Укажите все интересующие статусы сотрудников в компании, синхронизированные из TM или AD.

* - For attributes related to persons the following modifiers can be specified:

- *Any;*
- *Sender;*
- *Adressee.*

If you specify the modifier *Sender/Adressee*, selected persons or groups of persons will become senders or adressees of events.
If you specify the modifier *Any*, all the persons participating in event will be selected: all persons or groups of persons.

After the attributes values have been changed the following reports are automatically rebuilt in filter:

- diagrams, distributions and tables within **Statistics** section;
- events data tables within **Statistics** section;
- graphic display within **Connection graph** section.

To save specified filter attributes to be used in the future:

1. Click **Save** in the Single filter area.
2. In the opened window please specify the name of new filter.
3. Specify the type of filter:
   a.Personal - this filter will be available only for Security officer, who created it
   b. General - Filter will be available for all System users.
4. Click **Save**.

To use previously created filter:

1. Click **Requests** within th Single Filter area.
2. Cick on the required filter to enable it. Security officer is able:
   a.  - edit Personal filters and General filters.
   b.  - delete Personal filters as well as the General filters in case they were created by him/her previously.

If you require removing one filter from Single filter board, click  opposite the filter.

If you require clearing the filter values you have previously entered, open the filter clicking on its name and then click **Clear filter**.

Note:

You should take into consideration the following:

- all Single filter settings are applied within one browser tab only;
- when using next/back options (browser button Next/Back), a filter gets the status it had on a specified step;

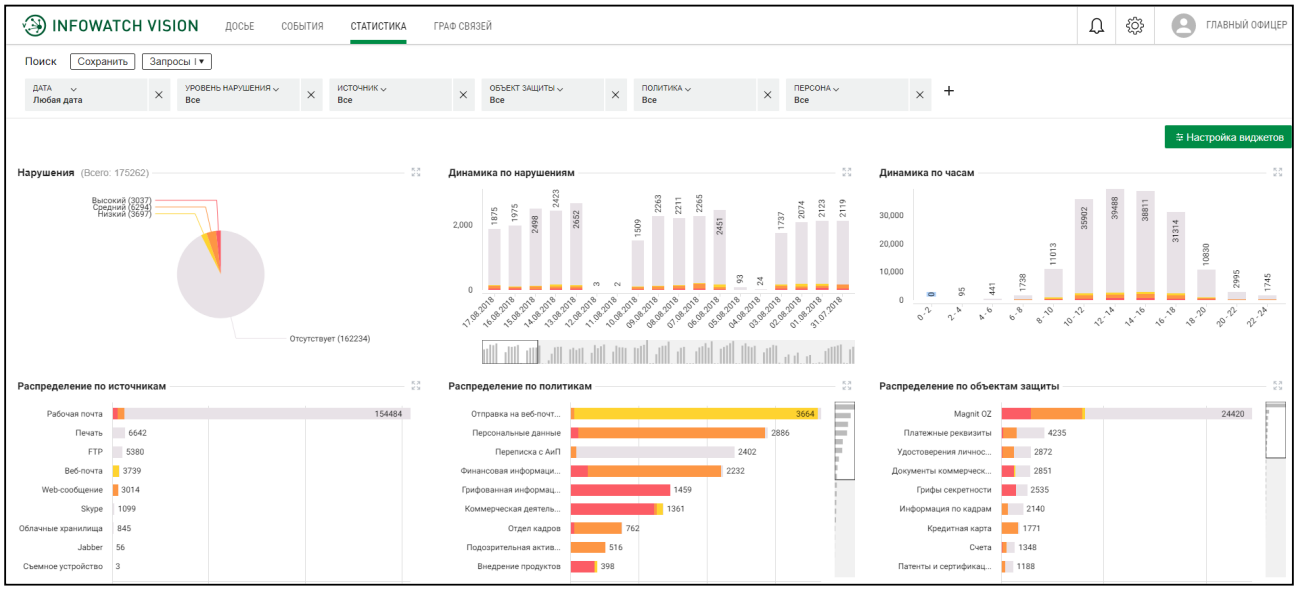
- when leaving the System, all filter attributes are dropped to initial state.

4.2 Statistics section

About this section:

This section contains statistical data of violations/violators. It is displayed on the widgets which are:

- convenient to use for daily monitoring;
- providing the fast review of events statistics.



Using the **Open fullscreen** button you may maximize the selected widget on the screen. To return to normal mode, click **Minimize**.

Workspace setting are used to:

- set widget size;
- specify widget location in the workspace.

To set up widgets displaying click **Setting widgets** and then:

1. If you require hiding a widget from workspace, click . If you require relocating a widget to a different part of display, drag and drop it to required area, holding cursor on a widget name.
2. Click **Save** to save the changes implemented.

To add a widget:

1. Click **Setting widgets** -> **Add widget** in the right corner of the working area.
2. In the opened window click **Add widget** opposite the widget you require. Click **Cancel** if you've selected the wrong widget.
3. Confirm the input by clicking **Apply** and then click **Close**. The new widget will be added in the working area. If apply is not required, click **Cancel**.
4. Click **Save** to leave widgets managament mode. All changes you've implemented will be saved.

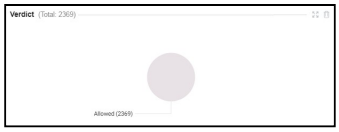
To filter data on a widget according to required parameter:

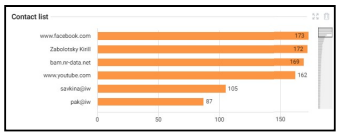
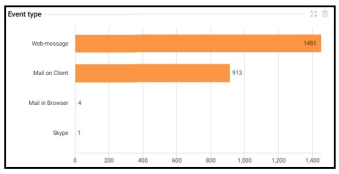
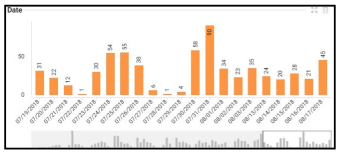
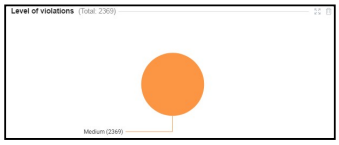
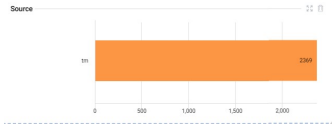
1. Specify required parameter on a diagram or click with the left mouse button on its description.
2. Click  in the corner of widget. Single filter parameters will be changed and displaying will be accordingly modified.

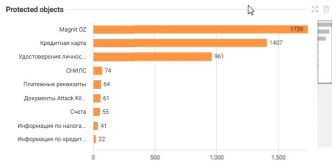
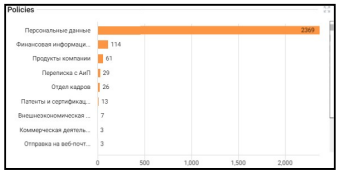
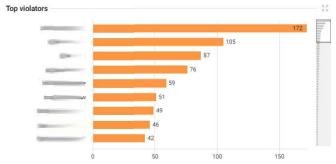
4.2.1 Statistics widgets

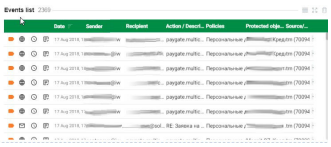
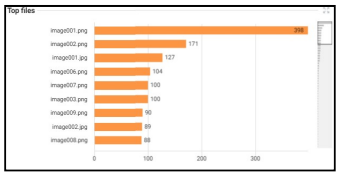
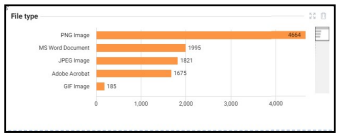
Widgets of **Statistics** section used to display the data stored in the Sytem:

<table>
<tr><th>Widget name</th><th>Description</th></tr>
<tr><td>Statistics

</td><td>Table view of data. When editing the widget you may select a value for row and select a value for column. Values for row are as follows: Policies, Persons, Source, Protected objects. values for cilumn are the following: violation level and type of event.
To set up the widget:
1. Click  in the top right corner of the widget.
Set the values as follows:
<table><tr><th>Parameter</th><th>Description</th></tr><tr><td>Select a value for a raw</td><td>You can select from the list:
• Persons ofe
• Policies
• Protected objects
• Source</td></tr><tr><td>Select a value for a column</td><td>You can select from the list:
• Violation level
• Type of event</td></tr></table>2. Set  opposite Show the total number of events to add Total column to the table.
3. Click Generate to prepare the table.
You can add few Statistics widgets, if required.</td></tr>
<tr><td>Verdict

</td><td>Used to display the differents of events by verdicts assigned by Security officer in Traffic Monitor. Each sector contains information about the number events with specific verdict which were downloaded to the System.</td></tr>
</table>

Widget name	Description
Contacts list 	Used to display the person's communications with all types of contacts: identified and unknown. The first 50 most popular contacts are displayed.
Event type 	Used to display different types of Traffic Monitor events. To get details When placing a cursor on a source name, you will see the details of events number with different violations levels as follows: 
Date 	Used to display events different by dates. You can specify one or few dates and filter the events in accordance with specified dates.
Level of violations 	Display the violations levels.
Source 	Displaying events differnt by system source.
Time 	Displaying the events distribution by day/night hours (every 2 hrs).

Widget name	Description
Protected objects  	Displaying eventys distribution with different violations levels as peк protected objects. The events is displayed within Statiastics if it contains any selected protected object. **Note:** If there are few protected object in event, it will be taken into consideration few times. Widget displays all protected objects filtered by Single filter from events. Thus, selecting one protected object as filter you can see the rest protected objects as well.
Policies  	Displaying events distibution with different violations types as per policies. To get the details When placing the cursor on any diagram rows area, you will see the information related to the number of events with different violations types were registered in the System in accordance with specified policy. **Персональные данные** High 0 Medium 2357 Low 0 No 0 **Note:** If you've applied few policies to one event, it will be considered few times. Widget displays all the events filtered by Single filter. Thus, selecting one policy as filter you can see the rest policies as well.
Top violators  	Displaying the list of persons whose violations are frequently registered by the Suystem. The first 50 top violators sorted by events with maximum violation levels are displayed.

Widget name	Description
Events list 	Displaying the list of eventrs extracted from Traffic Monitor in accordance with filtering, displayed via table. To get the details 1. Select one or few events, pressing *Shift* or *Ctrl* button. 2. Click  to the right within event line or click  . 3. Click **Go to event in source system**. A new tab will be opened in browser window displaying TM management console with an event which was previously synchronized.
Top files 	Displaying the list of files with violations intercepted by Traffic Monitor. The first 50 frequently met are displayed.
File type 	Displaying the events statistics in accordance with types of files (for example, images, text, media, etc.). A diagram column contains the number of events with this type of file.
Events list (short) 	Displaying the events in a table view (for more details please see "Events section").

Note:

To provide stable operation of widgets it is recommended to avoid complicated requests and to apply additional filters.

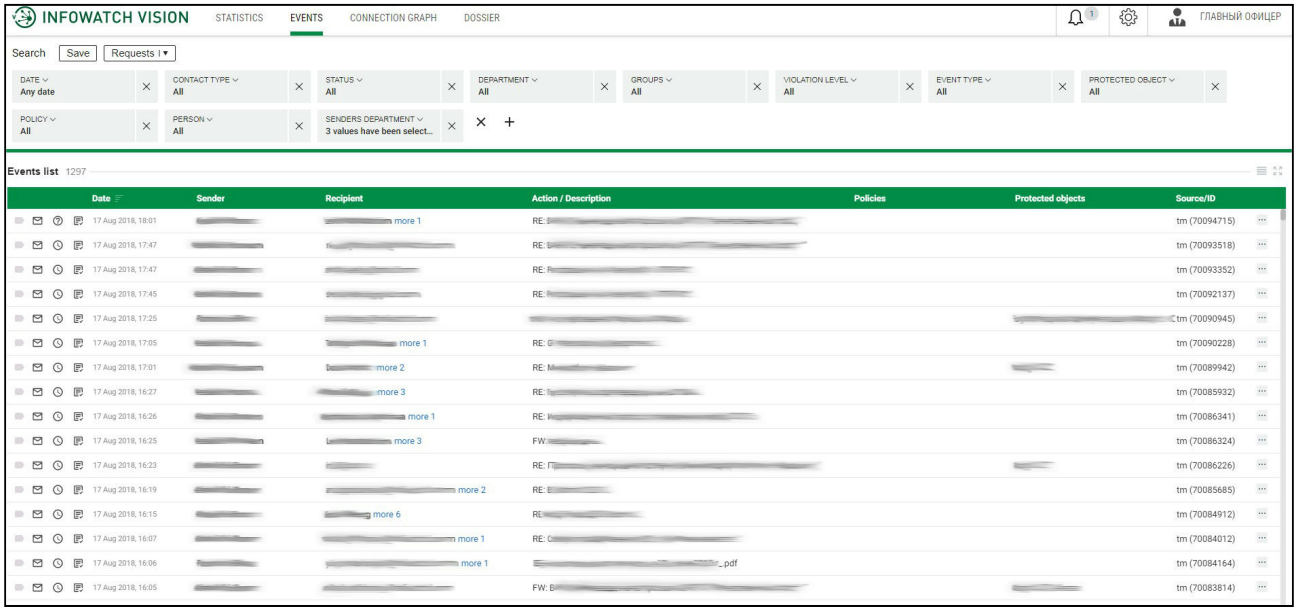
4.3 Events section

About this section:

In this section you may find all the data related to events downloaded to the System after it was synchronized with Traffic Monitor:

- violation level;
- event type;
- Security officer's decision on event;
- sending status;

- event creation date in Traffic Monitor;
- sender - a person who commited a violation;
- recipient - a person, receiving data from sender;
- sent data description and actions taken;
- policies, responded on this specific type of violation;
- protected objects which were sent;
- event ID in Traffic Monitor.



To get required events sampling a Security officer should configure filters on Single filter board (for more details please see "Single filter"). Security officer will get a list of events, where he/she can select few events and go to initial System to perform more detailed analysis. In case events belong to few sources, they will be displayed on different browser tabs.

To view event's data in initial System the following actions are to be taken:

1. Click ... opposite the required event.
2. Click **Go to event in source system**.

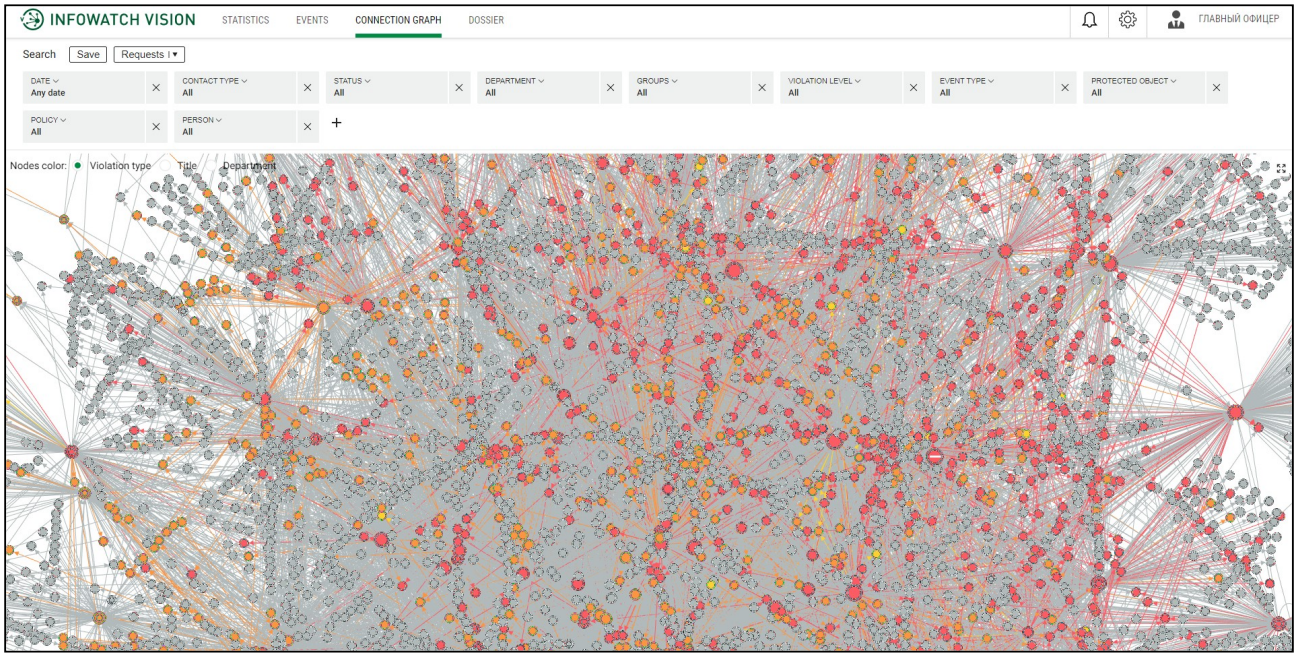
To view the data which belong to a group of events, select required events and click .

> **Note:**
>
> In order to work properly the System should be allowed opening popup windows from specified sources in browser.

4.4 Connection graph section

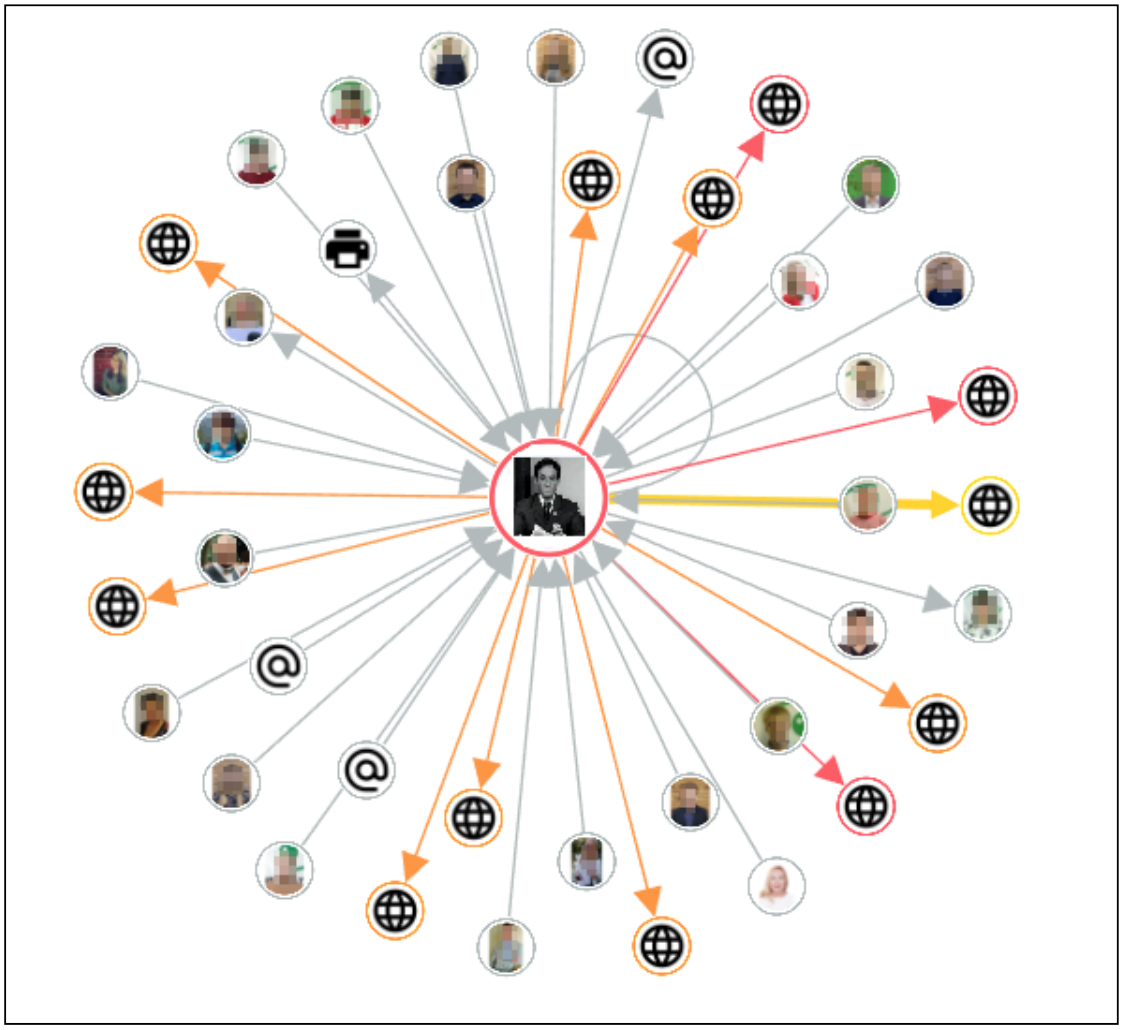
About this section:

This section contains the System data displayed on the screen via Connection graph which is built in accordance with the attributes values of Single filter.

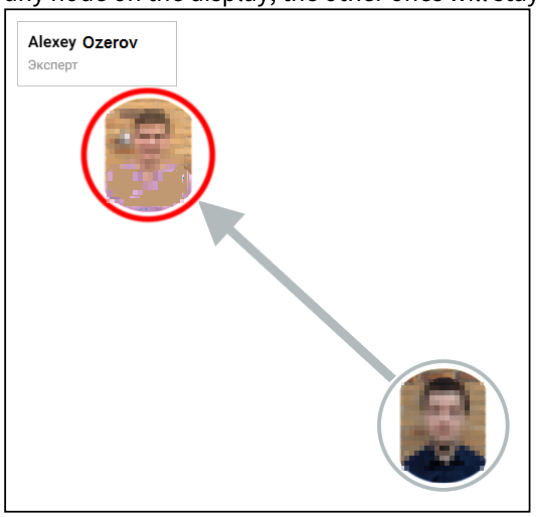


4.4.1 General information about graph

Connection graph in employee dossier is built in accordance with events where the employee was involved in as sender or adressee. Company's employees or resources are displyed on the graph via nodes, their connections are displayed via ribs.



Next to the rib you may find its name, containing the emplyee's name, name of resource and etc. Nodes are connected with different colour lines. Nodes are fixed on the graph and do not depend on each other. If you move any node on the display, the other ones will stay fixed.



The colour of a node can be set when using an additional filter and it is specified by the following data:

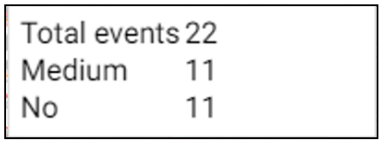
- maximum level of violation among all node's connections, in case the "Violation level" was specified;

- different persons affiliation to one company's department, in case the "Department" was specified;
- job title assigned to a person in the company, in case the "Title" was specified.

Nodes are connected between each other, two nodes has only one connection between them.

Connection parameter	Description
Connection line arrow	Used to show the data flow from nodes. It can be: • aimed to one side, in case the data flow is one side oriented; • with no direction specified, in case it was two-way data flow; • closed loop.
Connection line thickness	Depends on the number of events as per connection: the more events, the thicker line is.
Connection line colour	Defined in accordance with maximum violation level in connection events. The connection colours are defined as follows: • Red – high level; • Orange – medium level; • Yellow – low level; • Grey – no violation.

When you place a cursor on a connection line, you will see the number of events with violations levels graduation which were detected by Traffic Monitor.



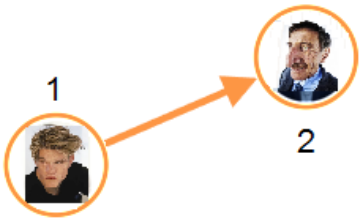
Events types are displayed on Connection graph via icons:

Icon	Description
	Web message
	Web mail
	E-mail
	Terminal session
	External devices
	Printers
	Cloud storage

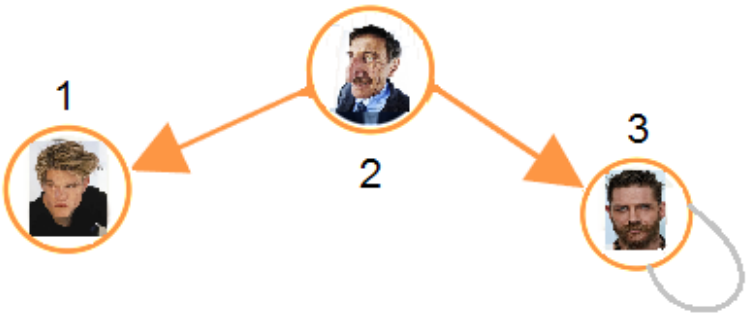
	FTP, Corporate network resources
	Messengers

4.4.2 Graph construction principals

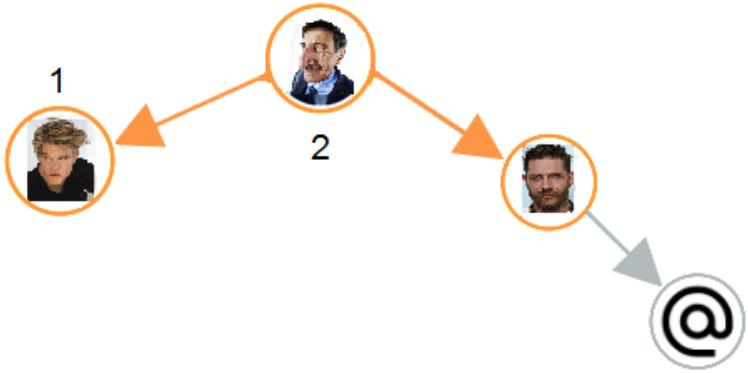
In the table below you may find the construction scheme of Graph connecting company's employees in accordance with scenarios used - from simple one (two employees) to complex scenario (big amount of nodes and connections).

Employees activities	Connection graph and description
1. Employee 1 sent e-mail to Employee 2 with attachments as follows: 1.dwg, 2.jpeg. 2. Traffic Monitor detected a violation of "drawing sending" policy for this event. A medium level was assigned to this violation.	 On the Graph you can see two nodes and connection between them. When moving a cursor to the node you will see the employee's name and surname. Inside the nodes you can see employee's avatars via icons the way they are identified in Traffic Monitor. Orange connection line between Employee 1 and Employee 2 means the violation level for this event is medium. Nodes Employee 1 and Employee 2 are coloured in orange, since the maximum level of violation between all the nodes on the Graph is "Medium".
1. Employee 2 repied in Skype via empty contract blank containing company's stamp and two PDF docuemnts. When sending the reply Employee 2 added Employee 3 to the copy of message. 2. Traffic Monitor detected a "legal information sending" policy violation in this event as well as protected object "Contract with requisites", protected object "Agreement with patners". A medium level was assigned to this violation.	 A new node was added, Employee 3 and there is a connection between this node and Employee 2. All connections and nodes remain coloured in orange since the maximum level of violation in connections has not changed.

1. Employee 3 sent CRM unloading file from his/her working e-mail to personal one.
2. Traffic Monitor detected a "Client information sending" policy violation. A low level was assigned to this violation.

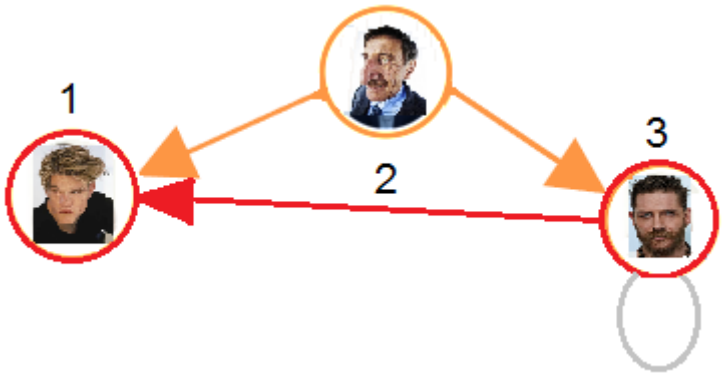


If employee's personal e-mail is identified by Traffic Monitor, then Employee 3 acquires a connection called closed loop. Loop (connection) is displayed in grey colour and the node Employee 3 is in orange, since he/she has obtained the connection (with Employee 2) with medium level of violation during the period specified.



In case his/her personal e-mail was not identified by Traffic Monitor, a new node with Unidentified contact" icon occurs.

1. Employee 3 sent e-mail with "xml. db" attachment to Employee 1.
2. Traffic Monitor detected a "DB sending" policy violation in this event and a high level was assigned to this violation.

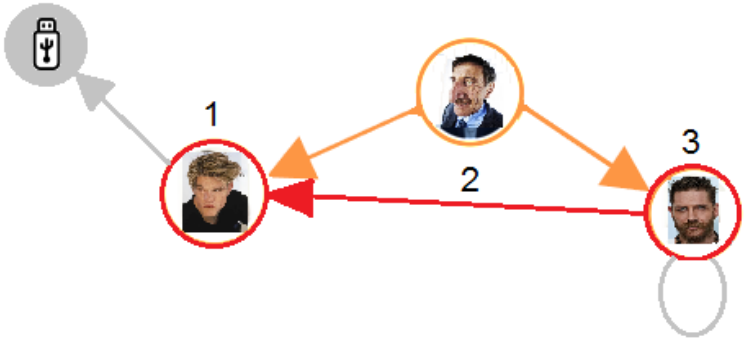


Nodes Employee 3, Employee 1 and their connections are displayed in red colour. If you filter the Graph by violation level "Medium only" then:

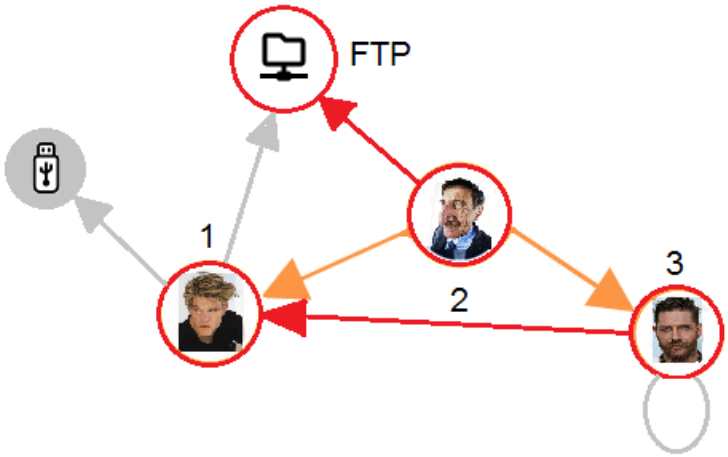
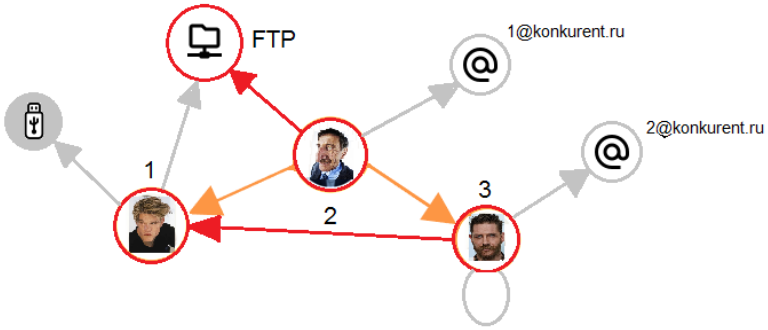
- only connections coloured in orange will remain;
- Employee's 3 closed loop will not be displayed;
- Employee 3 and Employee 1 nodes contours will remain coloured in red, since they have the connection with high level of violation during the period specified.



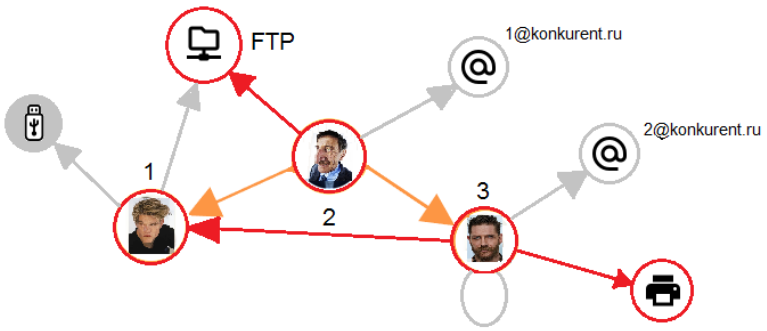
1. Employee 1 copied text file to external device..
2. Traffic Monitor did not detect any violation in this event.



On connection Graph Employee 1 has obtained a personal node "External device". Since there was no violation detected, the connection is coloured in grey. If Employee 1 will copy the data on a different external device, a new Graph will not be added to event. Each employee has only one personal node "External device" displayed.

1. Employee 1 copied file to FTP server. 2. Employee 2 copied file to FTP server. 3. Traffic Monitor detected a high level of violation from Employee 2.	 General node "FTP is displayed on the graph and its connections with Employee 1 and Employee 2. The node's size is growing in accordance with number of files copied to. Employee's 2 node and his/her connection with FTP are becoming red. "FTP" node will be added to Single filter in accordance with events types.
1. Employee 1 sent e-mail to competitive company's address 1@konkurent.ru. 2. Employee 2 sent e-mail to competitive company's address 2@konkurent.ru.	 On the Graph you can see connection nodes between Employee 1 and 1@konkurent.ru, Employee 2 and 2@konkurent.ru. 1@konkurent.ru and 2@konkurent.ru nodes icons are showing these nodes as "Unidentified contacts".

1. Employee 3 printed a file with copy of Russian passport.
2. Traffic Monitor detected a "Clent's personal data printing" policy violation in this event and a high level was assigned to this violation.

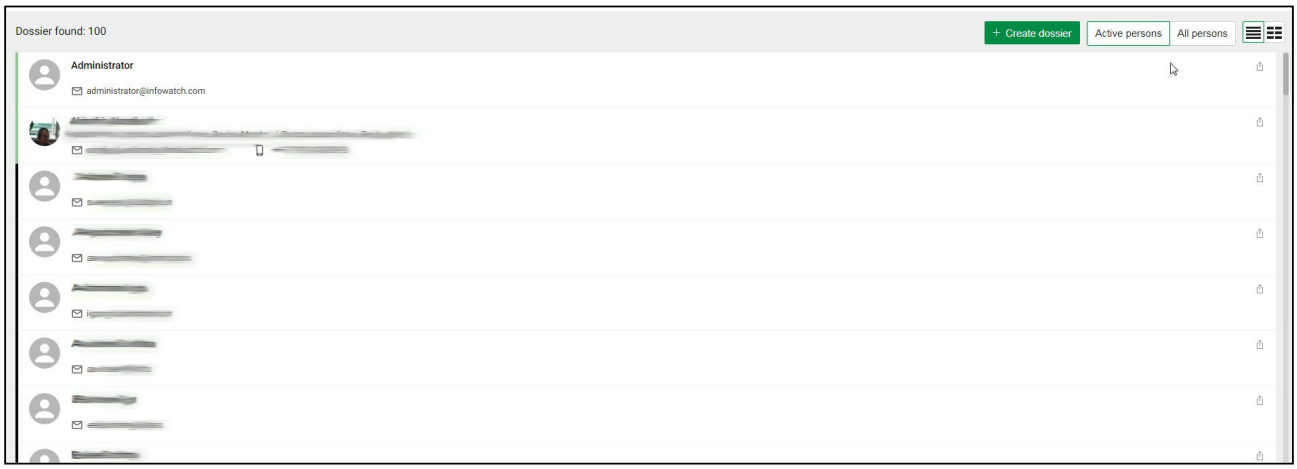


On Employee 3 Graph there is a personal node called "Printer". Employee 3 node and Printer are displayed in red colour. If Employee 3 prints the document on a different printer, tne node will not be added to "Printer" connection Graph. The connection "Printer - Employee 3" will become thicker due to events number growing. Each employee has only one personal node "Printer" displayed.

4.5 Dossier section

About this section:

This section contains contacts directory downloaded into the System when synchronizing with sources: Active Directory and Traffic Monitor as well as the persons manually added.



The persons table displays only the persons in accordance with Single filter requirements. To display persons dossiers you should use the toolbar on the right side of the working area:

- **Active persons** - displaying dossiers of employees with active accounts in active Directory;
- **All persons** - displaying dossiers of all the persons, including the ones ever working in the company;
-  - list view displaying;
-  - table view displaying.

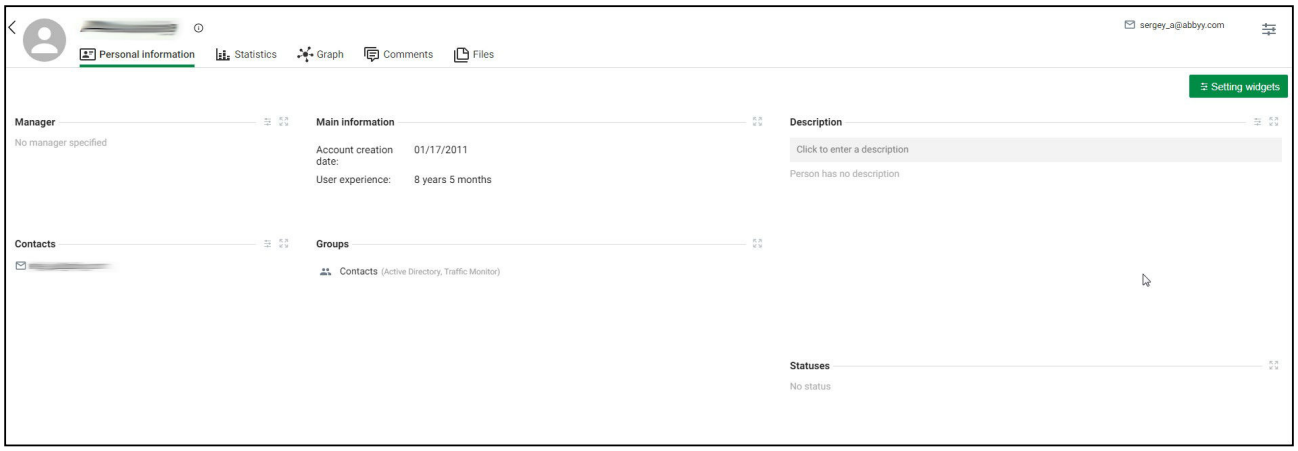
User functional activities:

- Person's dossier review
- Dossier creation, editing and deletion
- Dossiers merging

- Adding person's contacts
- Changing person's manager
- Person's connection graph
- Commenting person's dossier
- Adding file to dossier
- Dossier widgets

4.5.1 Person's dossier review

Dossier is a tool intended to collect and analyze data as per specific person. Dossier is used to organize common activity for few Security officers when exchanging information via comments. To review person's dossier click the left mouse button on the person specified within **Dossier** or **Events** sections. Person's dossiers contain the following tabs: **Personal information**, **Statistics**, **Graph**, **Comments**, **Files**.



On the page of person's dossier you can find employee's personal information:

- Employee's full name;
- Job title;
- Department;
- Contacts - personal and working contacts, including e-mail, telephone number, Skype login details, ICQ or web address.

For persons, whose data was imported from Active Directory the colour indicator is displayed in the top left corner of profile photo:

- - for active employees, including the ones with expeired ActiveDirectory accounts;
- - for employees, disabled in Active Directory.

To change the attributes specified above, including Name, Surname and photo editing use button in the right working area (for more details please see " Dossier creation, editing and deletion").

On the tab **Personal information** you can find Dossier widgets specific for this person. You can also add general Statistics widgets.

On the tab **Statistics** you can see statistics widgets related to this person (see "Statistics widgets").

On the tabs **Comments** and **Files** you can leave text notes and download files. This information will be added to person's dossier.

To return to the list of persons, click

in the top left corner of the working area.

4.5.2 Dossier widgets

Widgets are used to review all the person's data stored in the System. The table below describes the widgets specific for Dossier section. Also you can add generals statistics widgets on the tab Statistics in Dossier section (see "Statistics widgets").

Widget name	Description
Files	Displaying files related to a person and downloading new files to dossier.
Manager	Displaying a list of person's managers and setting a manager manually.
Contacts	Managing person's contacts and displaying contacts loaded from connected sources.
General information	Dispaying person's information provided by different sources.
Description	Displaying person's description, loaded from different sources and adding user attributes.
Statuses	Displaying a list of statuses assigned to a person in Traffic Monitor.
Comments	Adding comments to dossier.
Groups	Displaying a list of ActiveDirectory and Traffic Monitor groups, where a person is a member.

Widget's information can be stored in person's dossier. To do this the following actions are to be taken:

1. Click  on the required widget.
2. in the opened window leave a comment or download a file.
3. Click **Save**. All the information will become available in the tab **Comments**.

4.5.3 Adding person's contacts

When synchronizing with Traffic Monitor or Active Directory the person's contacts will become available: working and personal telephone numbers, e-mails, social networks accounts, etc. You can also add additional contacts manually. To do this the following actions are to be taken:

1. Go to person's dossier.
2. On **Contacts** widget click .
3. in the opened window you will see all person's contacts and types of connections. Click **Add contact**.
4. Specify the type of contact (for example, personal telephone number) and enter it. You can add few types of data or leave a comment related to a contact.
5. Click **Save**. New contacts will become available in dossier. If you leave a comment, next to contact you will see the icon . To read comments, click on this icon with the left mouse button.

4.5.4 Dossiers merging

Security officer has an option to merge two or more dossiers into one. The new dossier will include all the data from initial dossiers. To do this please take the following actions:

- Open the first dossier which is required to be merged;
- Click  and select **Combine dossier with...**;
- Select the second dossier from the liist. If required, select few dossiers;
- Click **Combine**.

4.5.5 Dossier creation, editing and deletion

To create a dossier for a new person and to create additional dossier for an existing person you should do the following:

1. Go to **Dossier** section.
2. Click **+Create doccier**.
3. Enter the personal information as follows:

Column	Description
Surname	Person's surname
Name	Person's name
Middle name	Person's middle name (if any)
Title	Job title within the organization
Department	Department where the person is assigned to
Description	Additional description
Photo	Add the person's photo

4. Add person's contact data including personal telephone number or working extension, e-mail address, social network account.
5. Click **Create dossier**. The new dossier will become available in the list of all employees dossiers.

To amend the dossier please do the following:

1. Open the required dossier.
2. Click  and select **Edit**.
3. Revise the data and click **Save**.

To delete the dossier, please do the following:

1. Open the required dossier.
2. Click  and select **Delete**.
3. Click **OK**. The dossier will be deleted with no option for restoration.

4.5.6 Changing person's manager

On the tab **Personal information**, widget **Manager** you can see the data related to person's manager. This information is provided from person's card in a source: ActiveDirectory or Traffic Monitor.

Security officer can change the manager manually. To do this the following actions are to be taken:

1. Cick .
2. In the opened window **Change manager** enter the name of new manager from the list of persons registered in the System to the field *Manually added.* Entering few names is possible.
3. Click **Save**. Now specified managers are displayed on the widget **Manager**.

You can also see the company managers hierarchy. To do this, click on person's manager name with the left mouse button thus following to his/her manager's dossier page.

4.5.7 Person's connection graph

Graph, the person's dossier tab displays a connection graph built in accordance with events related to this person. For more details please see Connection graph section.

Security officer can save person's connection graph. This can be used to prepare a report. To do this the following actions are to be taken:

1. Go to **Graph** tab within person's dossier.
2. If required, edit the graph.
3. Click .
4. In the opened window leave a comment.
5. If required, add the files, to do this:
   a. Click .
   b. Select the files and drag and drop them in the area using the mouse.
6. Click **Save**. The person's connection graph will be saved as a separate file. You can view this info in **Personal information** tab in **Comments** widget.

4.5.8 Commenting person's dossier

On Comments tab within the person's dossier you can leave your comments related to this person, as well as the files of different formats and a text. All these data can be used during the investigation or when preparing a report.

The tab contains the list of comments which can be sorted using specific key. To do this, select **Show new comments first** or **Show old comments first**.

To enter a new comment:

1. Click **Add comment**.
2. Input the data. If required add an enclosed file.
3. Click **Save**. The new comment will be displayed in the list as well as on **Comments** widget of **Personal information** tab.

To revise the comment:

1. Click  opposite the file.
2. Make changes.
3. Click **Save**.

4.5.9 Adding file to dossier

On **Files** tab in person's dossier you can add different formats of files or a text. All these data can be used to perform investigation or to prepare a report.

The tab contains the list of files to be sorted by specific key. To do this, select **First uploaded** or **Latest uploaded**.

To upload new file to dossier:

1. Cick **Add file**.
2. Add file, it will be available in the list of attachments.

Any Security officer can review the list of files previosly downloaded to the System. to do this:

1. Click  opposite the file.
2. Select **Download** or open the file to revie clicking with the left mouse button on its name.

If you require deleting the file:

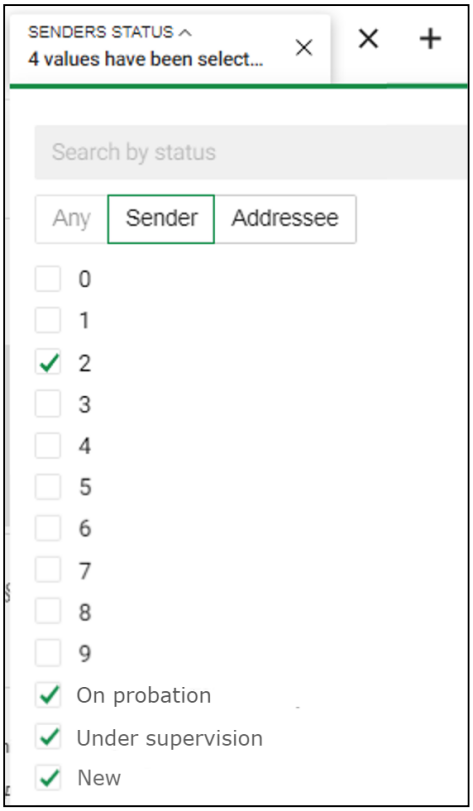
1. Click  opposite the file.
2. Select **Delete**.
3. In the opened window click **OK**.

5 Security officer operational scenario cases

5.1 Daily communications analysis for specified employees

To monitor the new employees activities on a daily basis Security officer can do the following:

1. Enable **Senders status** filter in **Statistics** section, selecting the values he/she requires.



2. Save the filter since it can be often used.



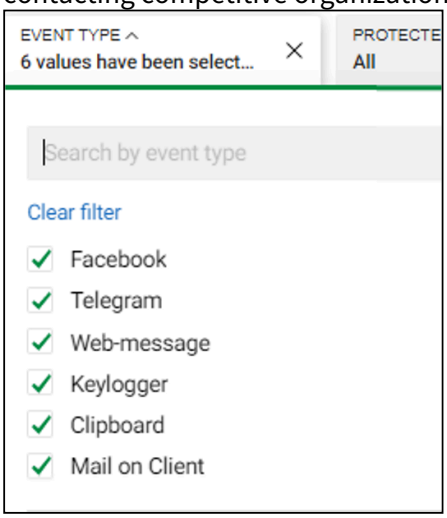
3. The filter you've saved will let you go to required events sampling fast and make your routinely activities simple.

5.2 Employee activity analysis

Once the company has an employee under suspicion, Security officer requires collecting maximum of information related to this employee. To do this:

1. Security officer is opening employee's dossier to analyze his/her activities as per suspicicious engagement: sending confidential data to external e-mails or saving it to removable devices,

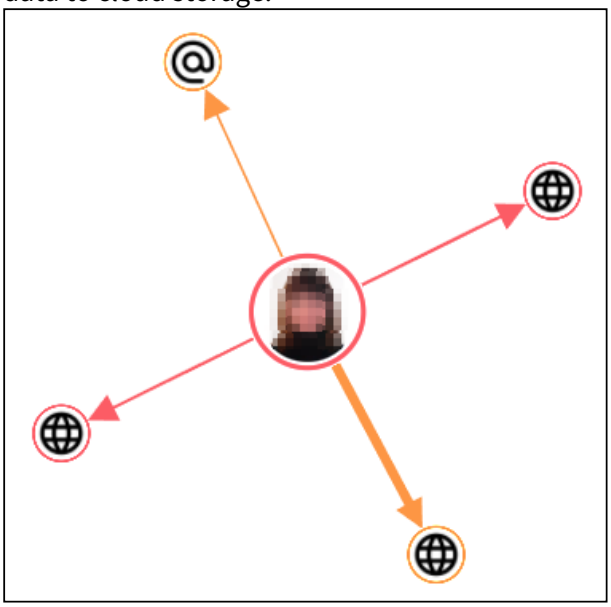
contacting competitive organizations or downloading big amount of files to cloud storage.



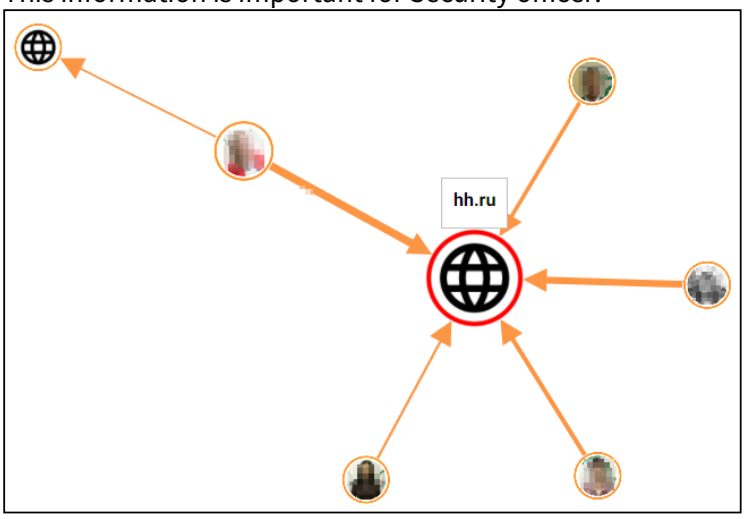
2. Security officer is specifying the leakage channels he is concerned about from the specified ones.



3. Security officer is detecting that these events have medium level of violation and are related to sending data to external e-mail. The employee also has a high level of violation related to sending data to cloud storage.



4. Further Security officer is deciding to check the company's loyalty towards this employee, if the user was trying to find another job.
5. Using TM policy "Job search" Security officer found few persons, who attended the related sites. This information is important for Security officer.

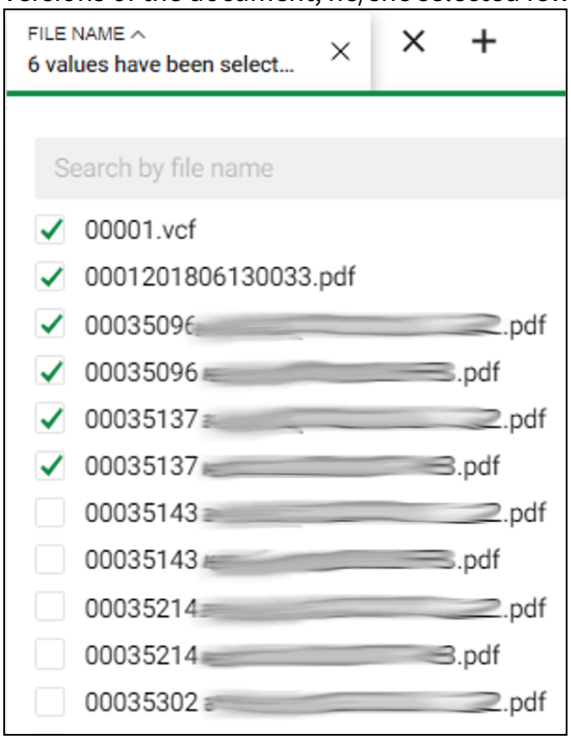


6. Security officer goes to **Dossier** section, **Graph** tab and saves it, attaching to dossier ( ).

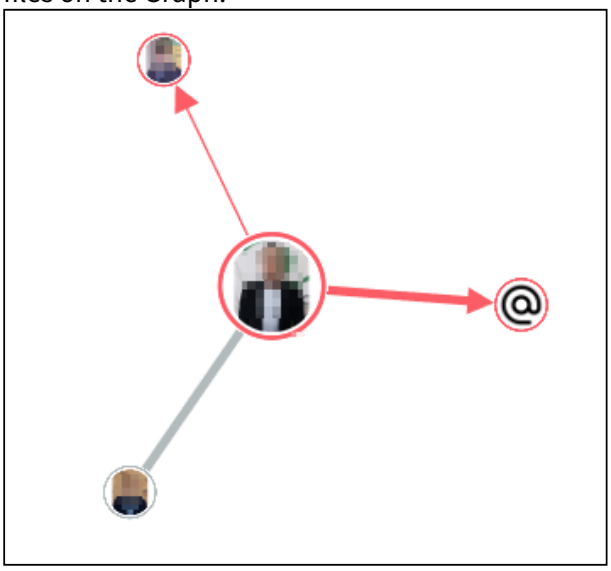
5.3 Detecting leakage channel

Confidential data was detected this month on a public resource. Security officer initiated an investigation to verify the employee who performed the leakage. To do this:

1. After the document content was analyzed, Security officer entered approximate name of the document to **File name** filter. The officer can see all similar documents which can be different versions of the document, he/she selected few files.



2. Security officer specified the time interval and then analyzed the persons exchanging specified files on the Graph.



3. Security officer detected leakage to external address, then going to **Events** section he/she researched in details all the source's events.

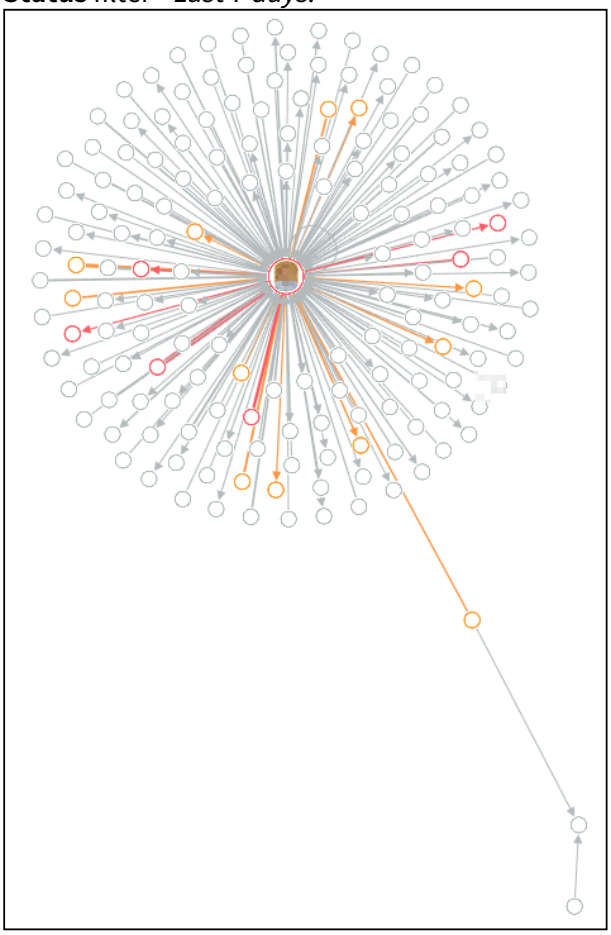
5.4 Specific employee communications analysis

Continous monitoring of specific personnel is also the responsibility of Security officer. Specific personnel include employees as folows:

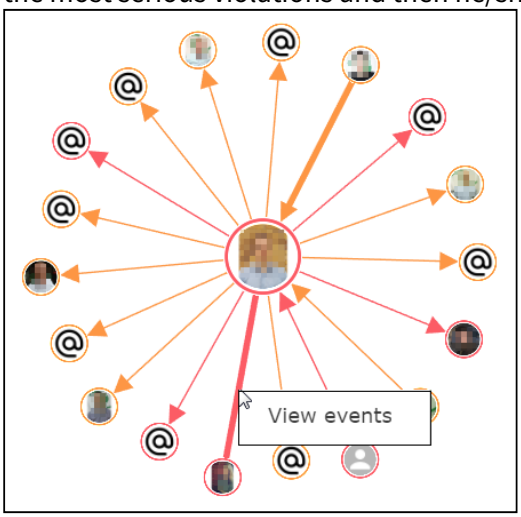
- recently recruited employees who are on probation;
- the ones who were suspected before;
- employees going to leave the company soon.

For this purpose:

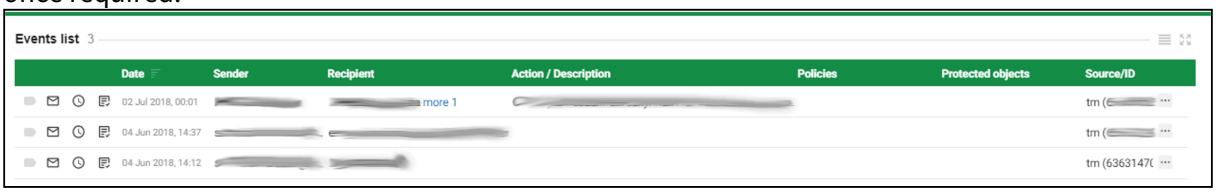
1. Security officer should open the section **Connection graph** and select *Under supervision* value in **Status** filter - *Last 7 days*.



2. Security officer applies additionally the filter **Violation level** in accordance with following values: *High*, *Medium* and *Low*. Graph is being rebuilt according to the filter. Security officer is able to find the most serious violations and then he/she initiates the events review.



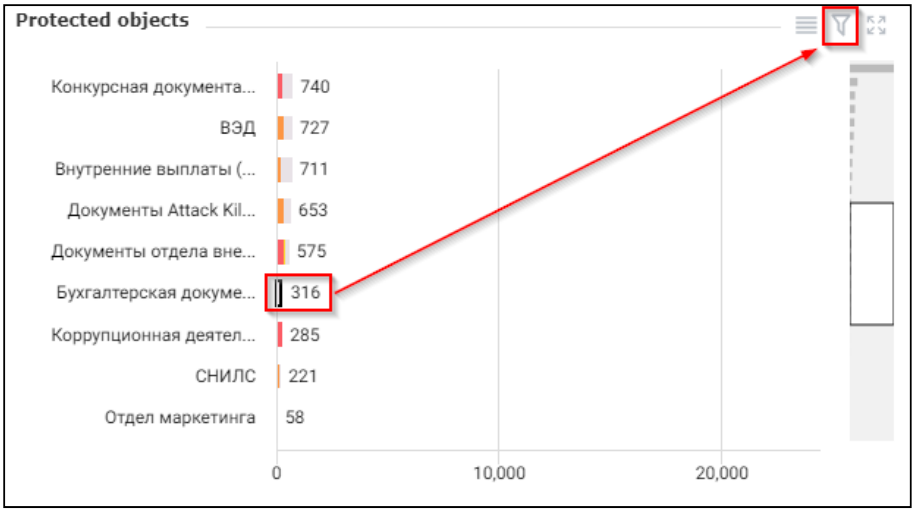
3. In **Events** section Security officer may review the events description and to view all the details once required.



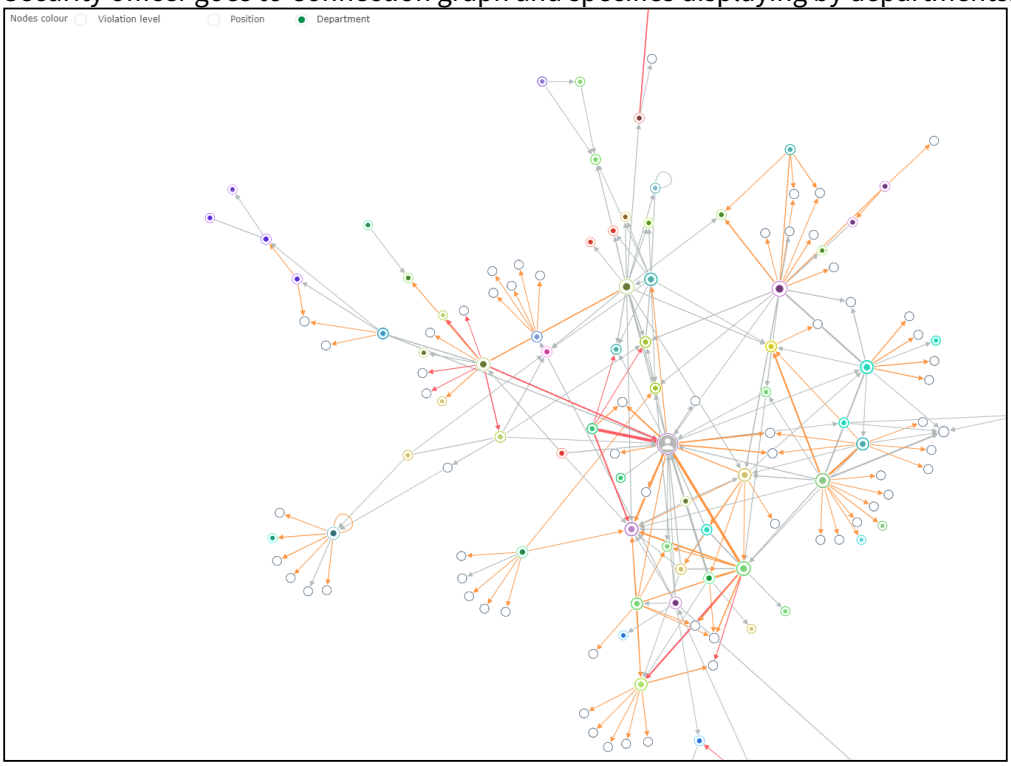
5.5 Analyzing company's business processes

Security officer requires to analyze the way some type of data (for example, Accounting documentation) is being extended over the company. This information will be used to configure security policies:

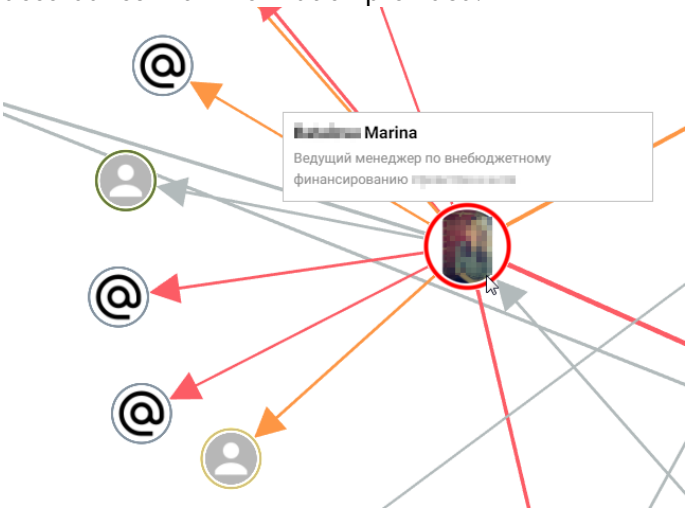
1. Security officer specifies **Бухгалтерская информация** as protected object and applies the filter.



2. Security officer goes to Connection graph and specifies displaying by departments.

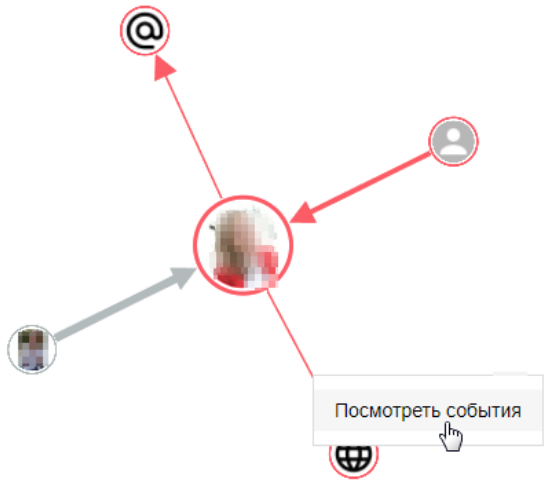


3. Security officer analyzes the main communication participants and set up security policies in accordance with information provided.

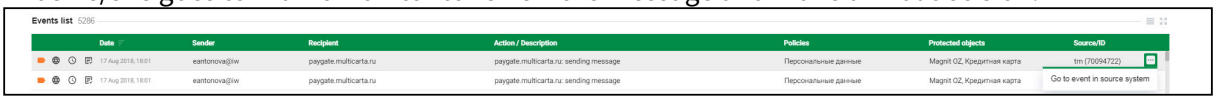


4. Security officer analyzes the information provided to verify if the data were illegally sent. He/she reviews all the graph elements, which relate to one sender and where the events are specified as incoming. As a result he/she detected a suspicious sending of accounting information (**Бухгалтерская информация**) to external server. Security officer selected the parts of graph

he/she is interested in the most and reviewed it.



5. On Events tab Security officer can see the emails subjects specifying sending to external server. Thus he/she goes to Traffic Monitor to review the message and make a final decision.

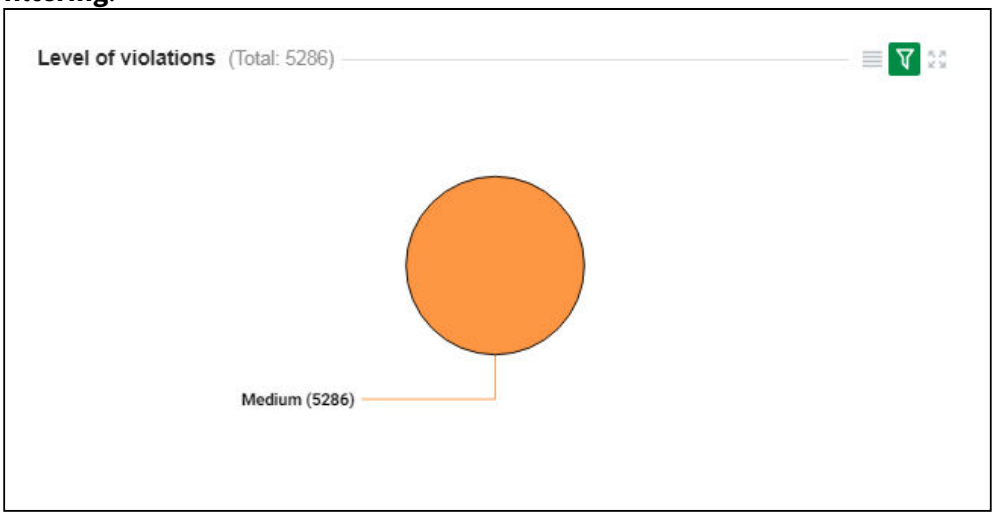


5.6 Fast search of anomalous employees conduct

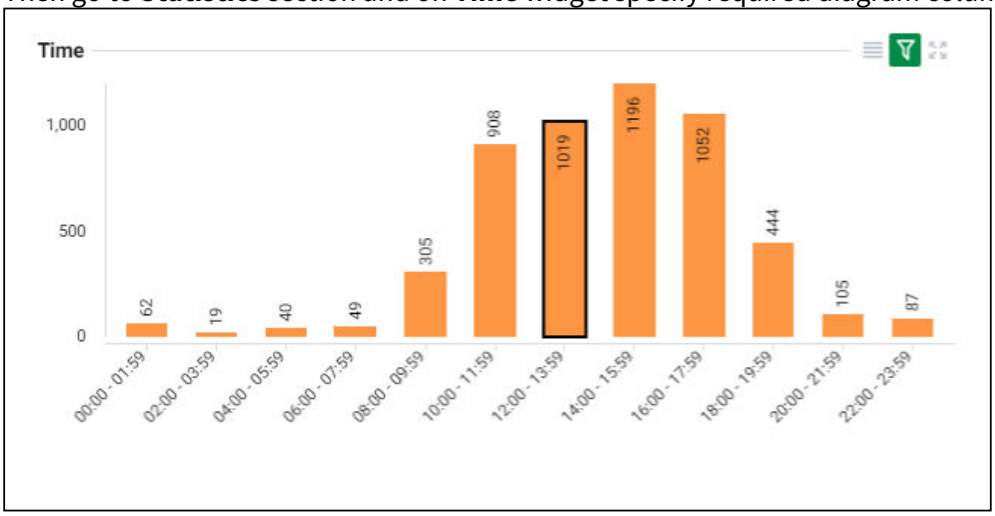
In some situations Traffic Monitor can detect the events related to atypical staff conduct.

To review the occasions specified above and to detect anomalies you should do the following:

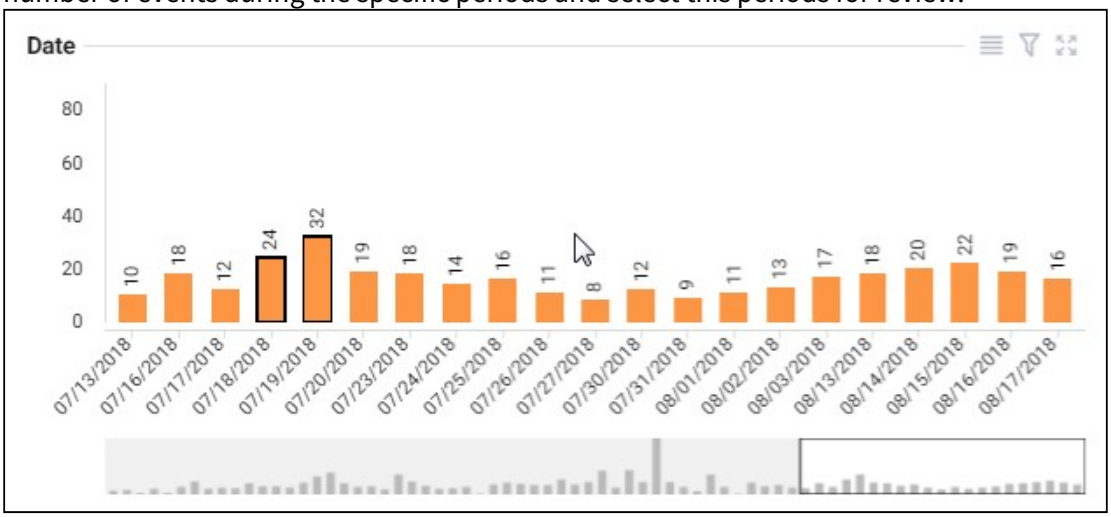
1. Go to **Statistics** section on **Violation level** widget select **Medium** levels of violation. Then click **filtering**.



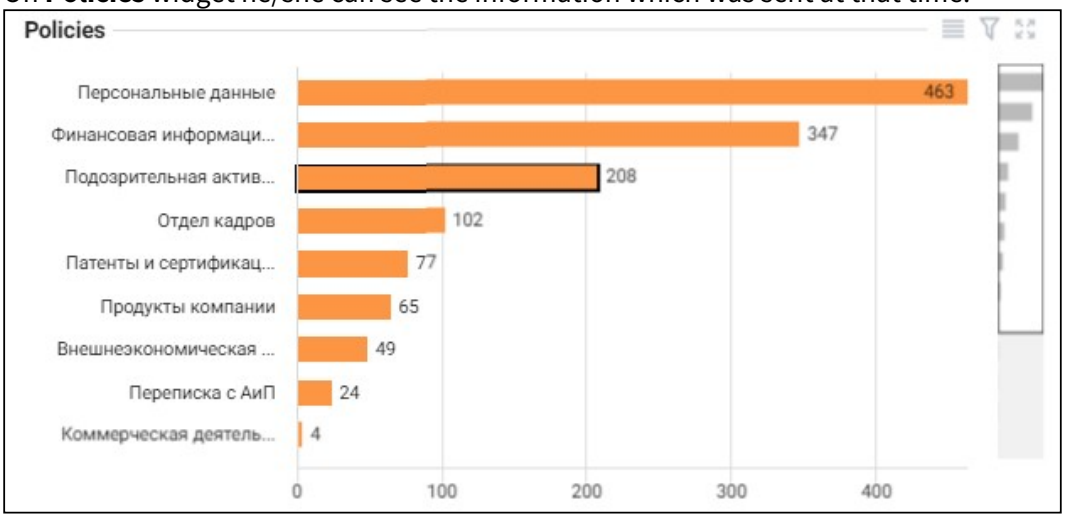
2. Then go to **Statistics** section and on **Time** widget specify required diagram column, click **filtering**.



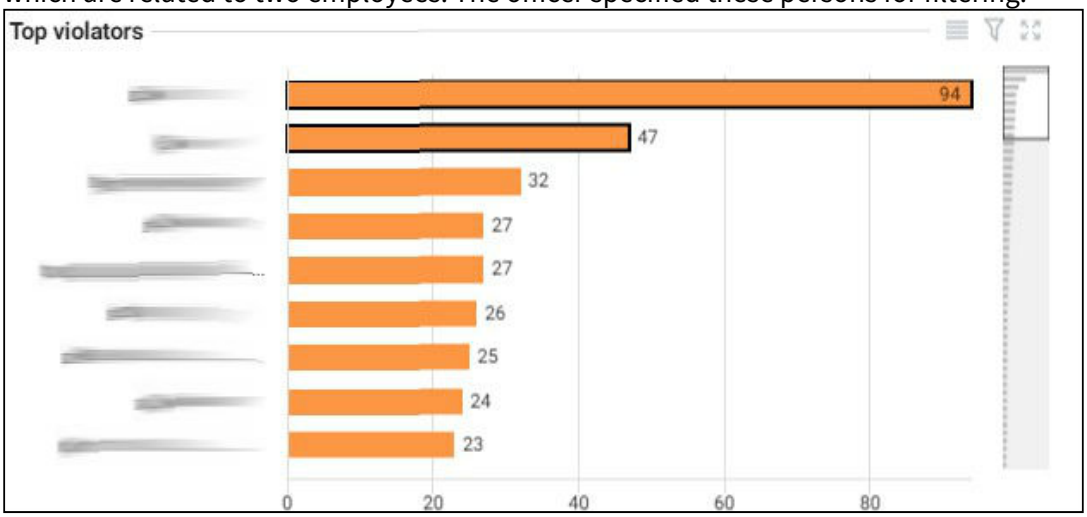
3. **Statistics** is being modified in accordance with new filter applied. Security officer can see the number of events during the specific periods and select this periods for review.



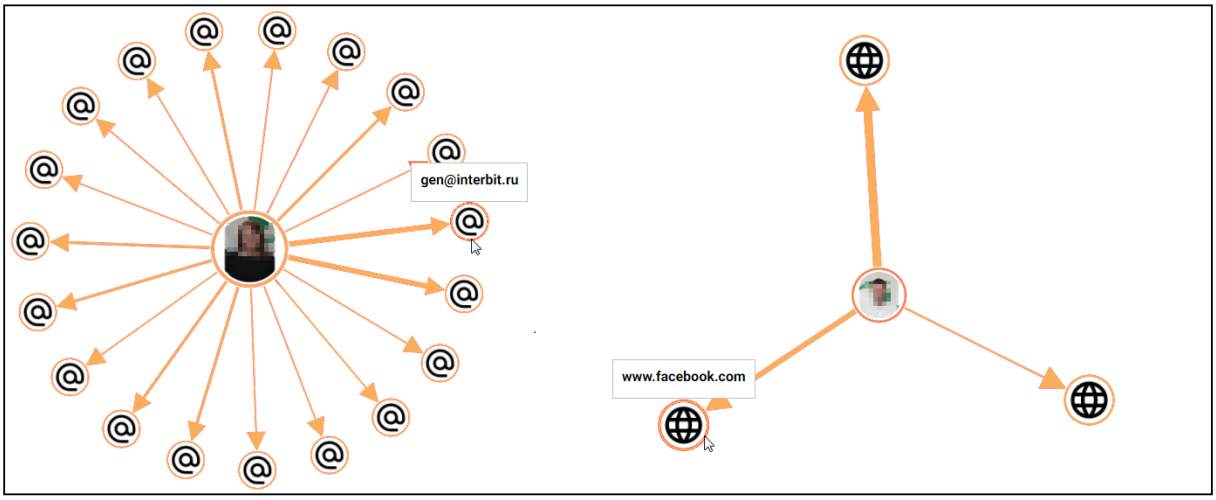
4. On **Policies** widget he/she can see the information which was sent at that time.



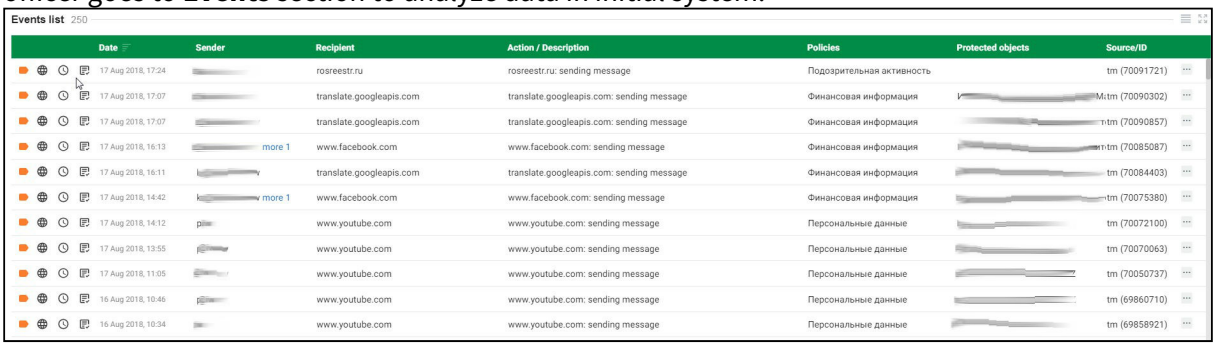
5. On **Top Violators** widget Security officer can see the list of violators and the main violations, which are related to two employees. The officer specified these persons for filtering.



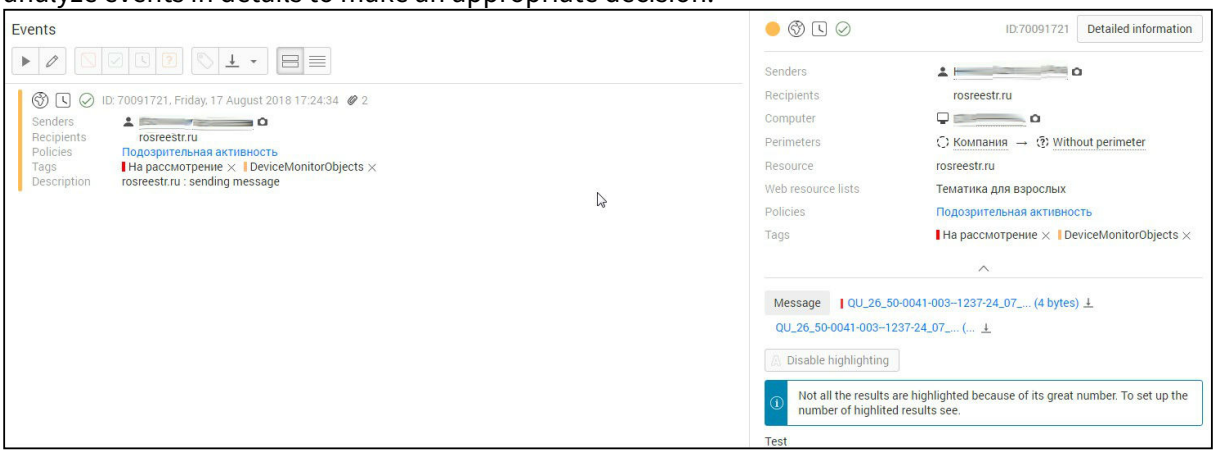
6. Then Security officer goes to **Connection graph** section and verifies the contacts of employees mentioned above.



7. Since sending personal data in non-working time to specified emails looks suspicious, Security officer goes to **Events** section to analyze data in initial system.



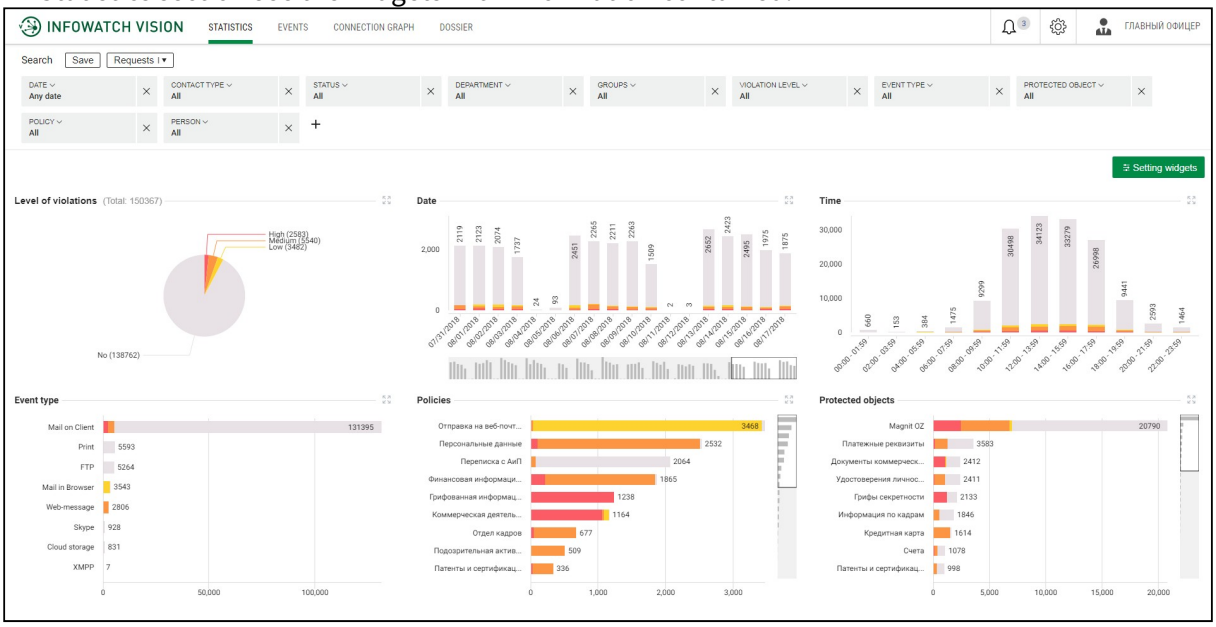
8. Selected list of events is displayed in Traffic Monitor standard interface and Security officer can analyze events in details to make an appropriate decision.



5.7 Collecting data to dossier

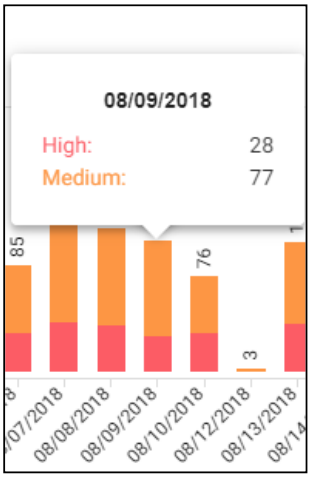
Collecting data is required to perform investigations and to prepare reports as per employees. Security officer can save all required data in employee's dossier.

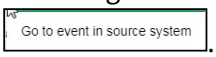
1. In Statistics section see the widgets with information contained.



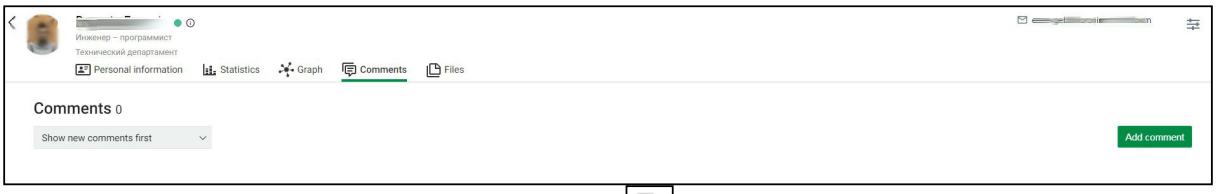
2. Find suspicious information or serious violations on the diagram.

3. Select it and click  to filter all statistics data.

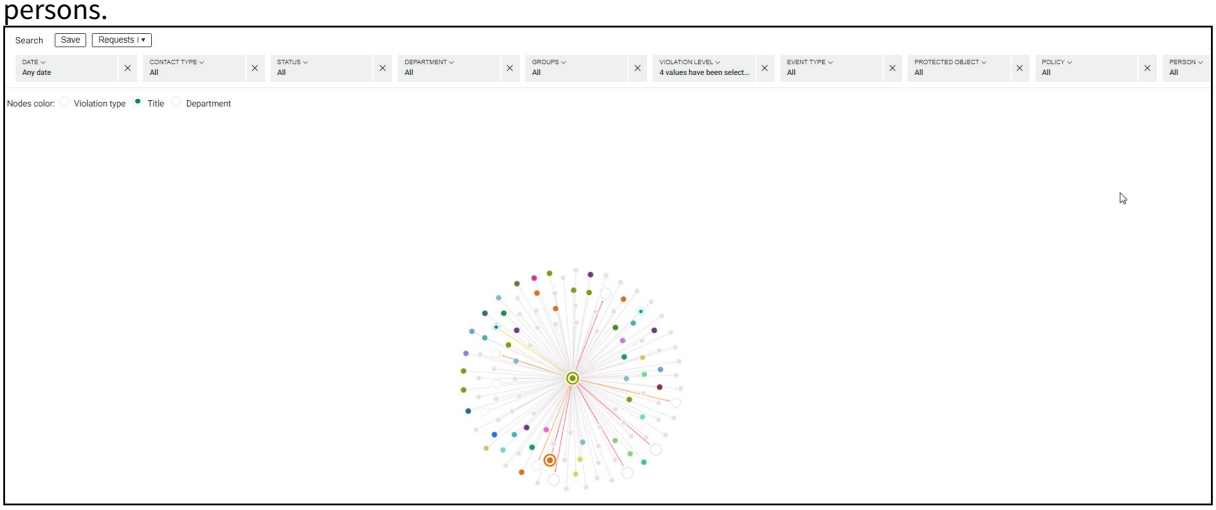


4. When the System displays required data, go to **Events** section.
5. You can go to the source system to review the details, in this case Traffic Monitor. Click and 

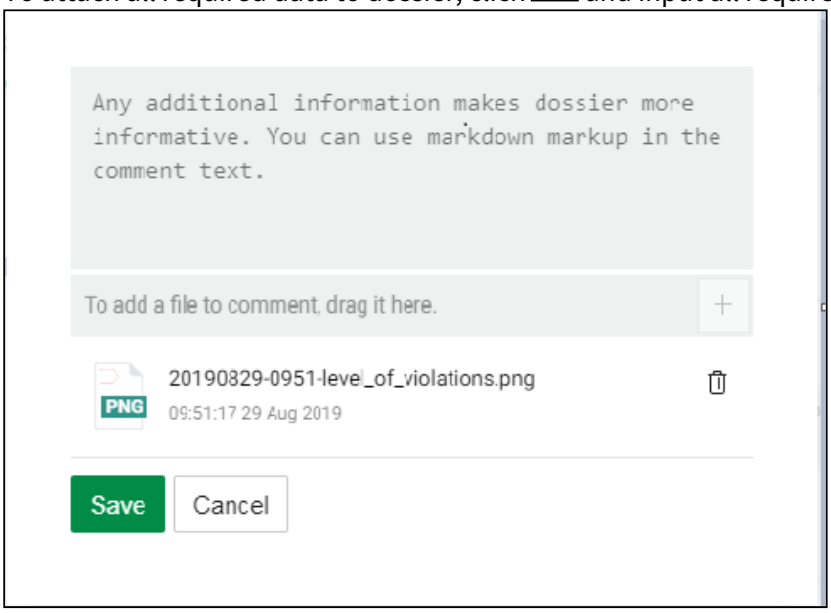
. You can see all filtered events by clicking .
6. After you've completed analyzing the events, go to specific person's dossier. To do this, click **Dossier**.
7. On dossier page within **Comments** tab leave all required information related to this employee and attach a file. To do this click **Add comment** and then click **Save**.



8. Go to **Statistics** tab. To save widget in dossier click  and input required data. Then click **Save**.
9. Go to Graph tab to review the information flows between this specific employee and other persons.



10. To attach all required data to dossier, click  and input all required data. Then click **Save**.



11. To add file to dossier, go to **Files** tab. Click **Add file** and attach the required file using file manager.
12. The System will download screenshot to a person's dossier. The system allows to restore context referring to the moment of the screenshot making. For details see "Commenting person's dossier".