MOSCOW FORENSICS DAY '25



ALEXEY DROZD

"USING STEGANOGRAPHY IN VARIOUS CHANNELS TO IDENTIFY THE SOURCE OF A DATA LEAK"
ИСТОЧНИКА УТЕЧКИ ДАННЫХ»

SEARCHINFORM LLC

MFD

SEARCHINFORM

USING STEGANOGRAPHY

in various channels to identify the source of a data leak



Alexey Drozd

Head of the Security Department
SearchInform

WHY?

Sometimes the security officer wants extra certainty about who the leak came from.

What can he do?



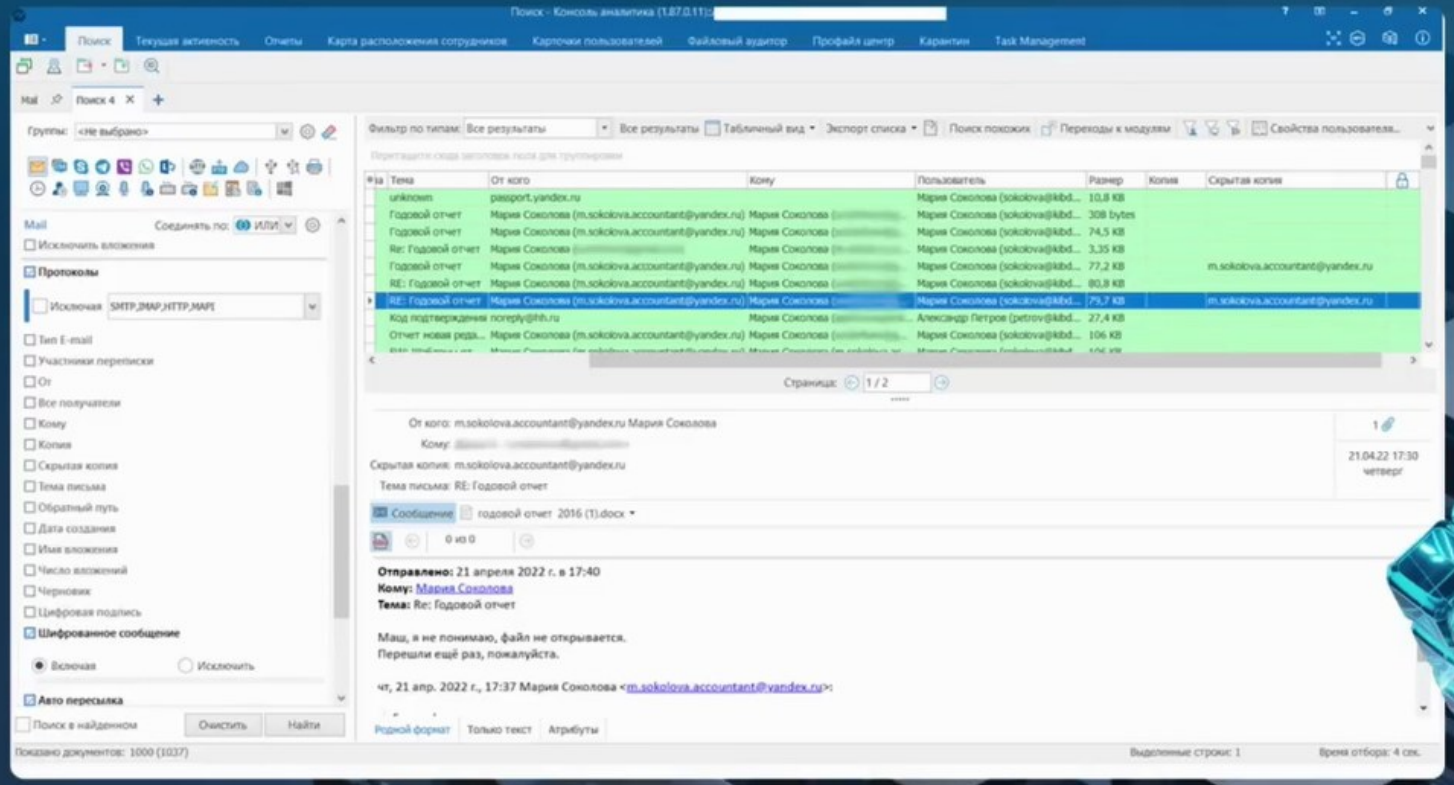
- IS-based approach
- File-based approach
- User-session-based approach

SEARCHINFORM

SEARCHINFORM

APPROACH BASED ON

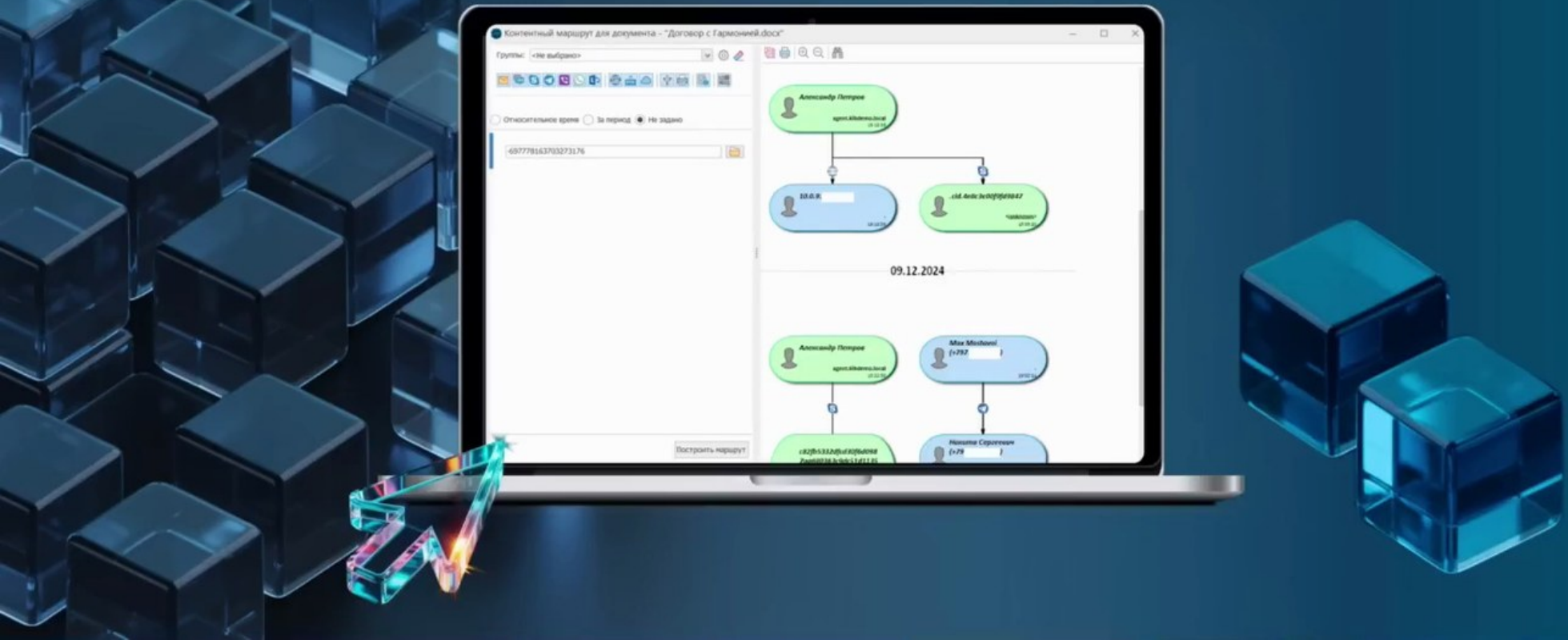
THE INFORMATION SYSTEM



SEARCHINFORM

APPROACH BASED ON

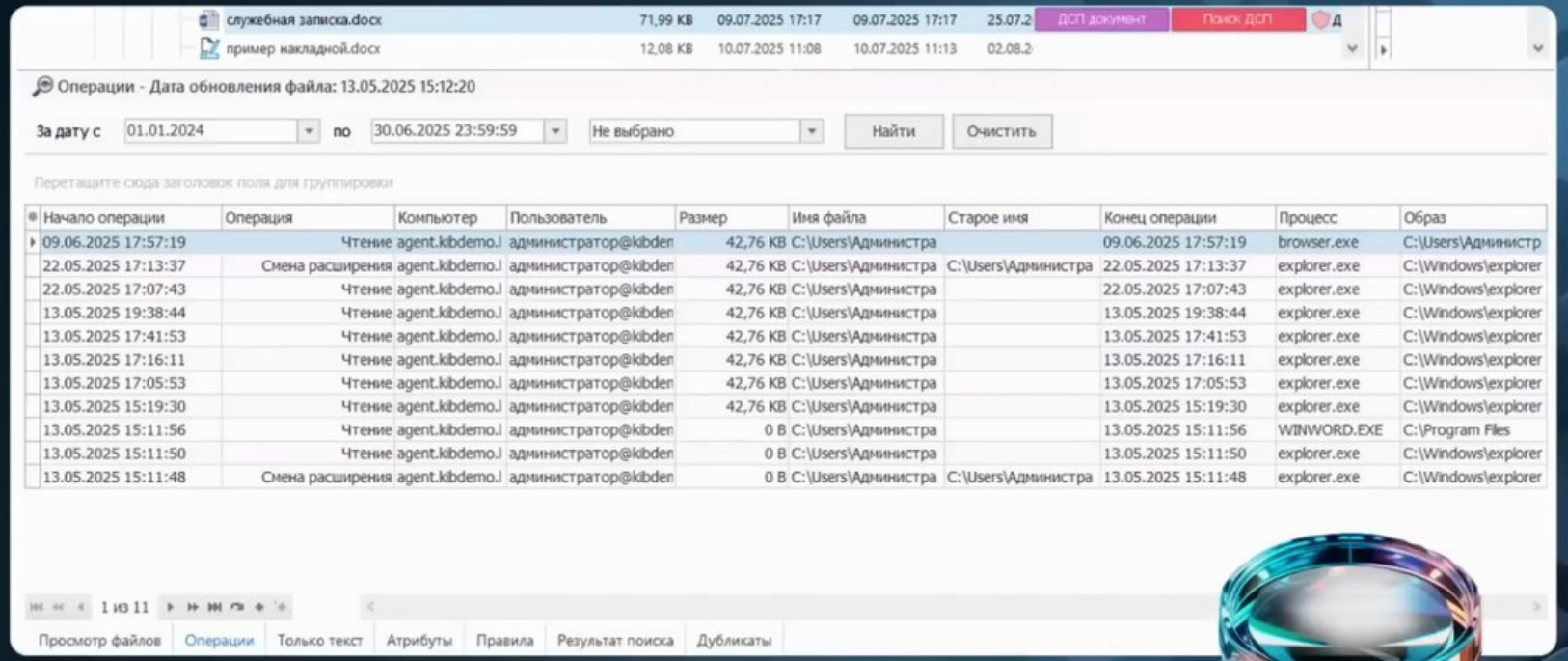
THE INFORMATION SYSTEM



SEARCHINFORM

APPROACH BASED ON

THE INFORMATION SYSTEM

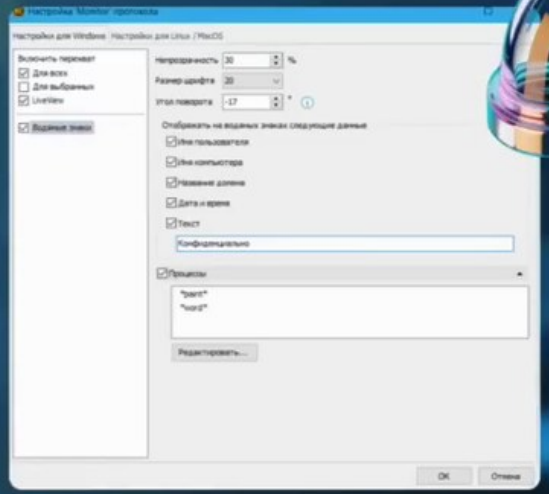


APPROACH BASED ON THE USER SESSION

Why?

Identifying the source of a data leak if someone filmed the screen or took a screenshot.







SEARCHINFORM

APPROACH BASED ON THE FILE

Why?

Identifying the source of a data leak if someone filmed the screen or took a screenshot.

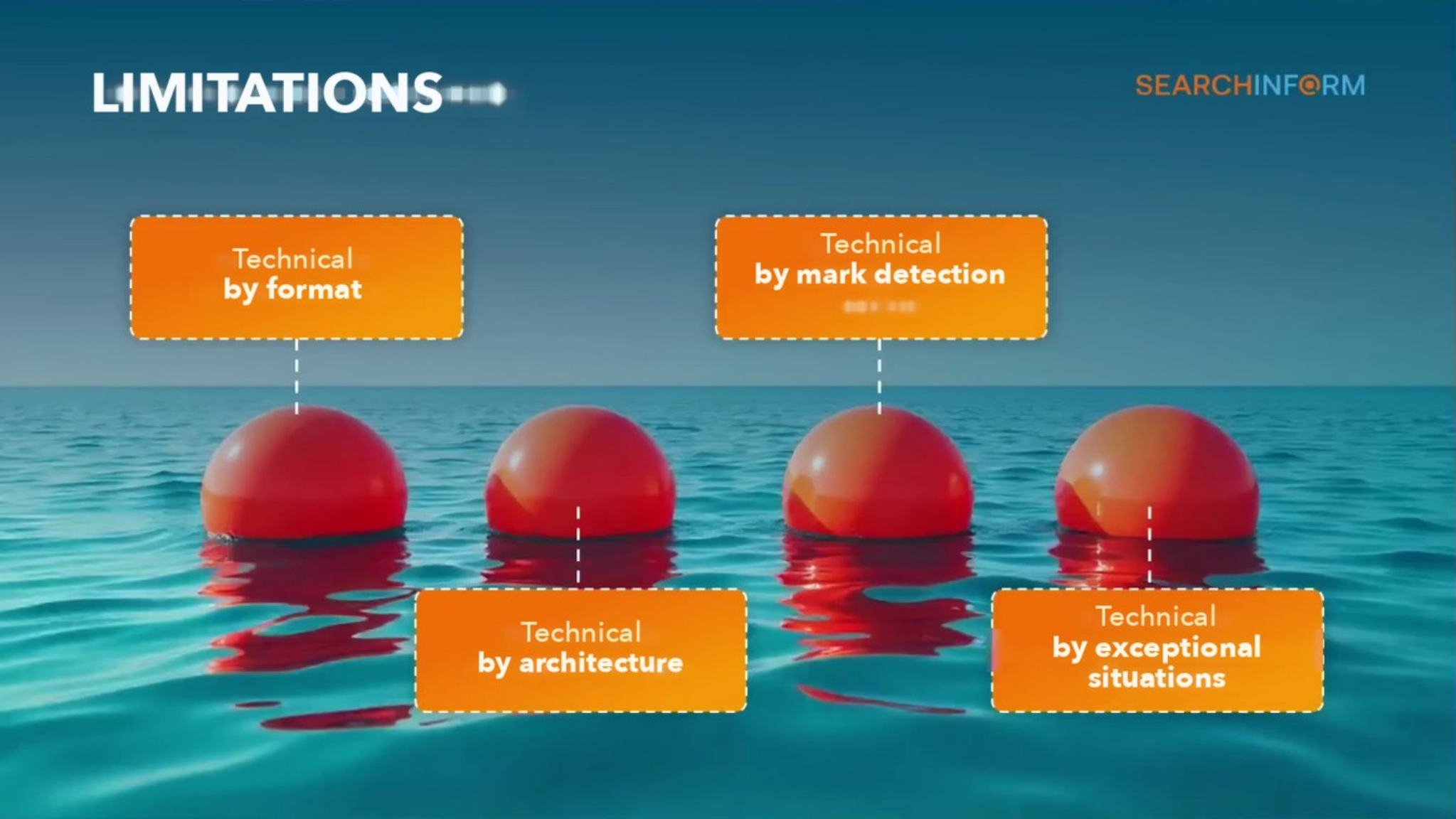




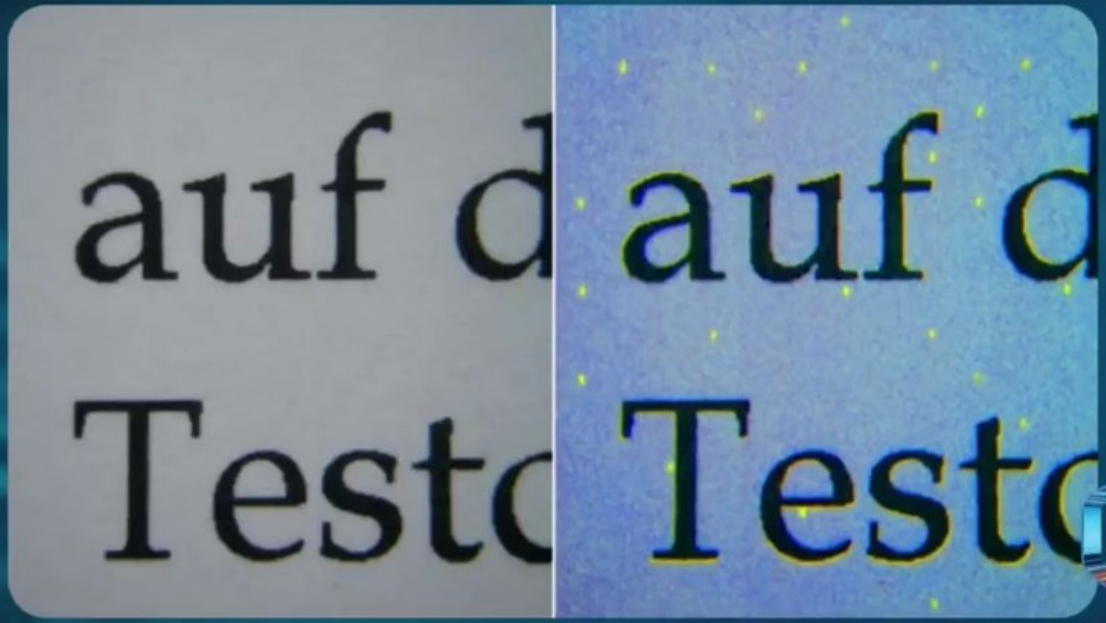
SEARCHINFORM

LIMITATIONS

SEARCHINFORM



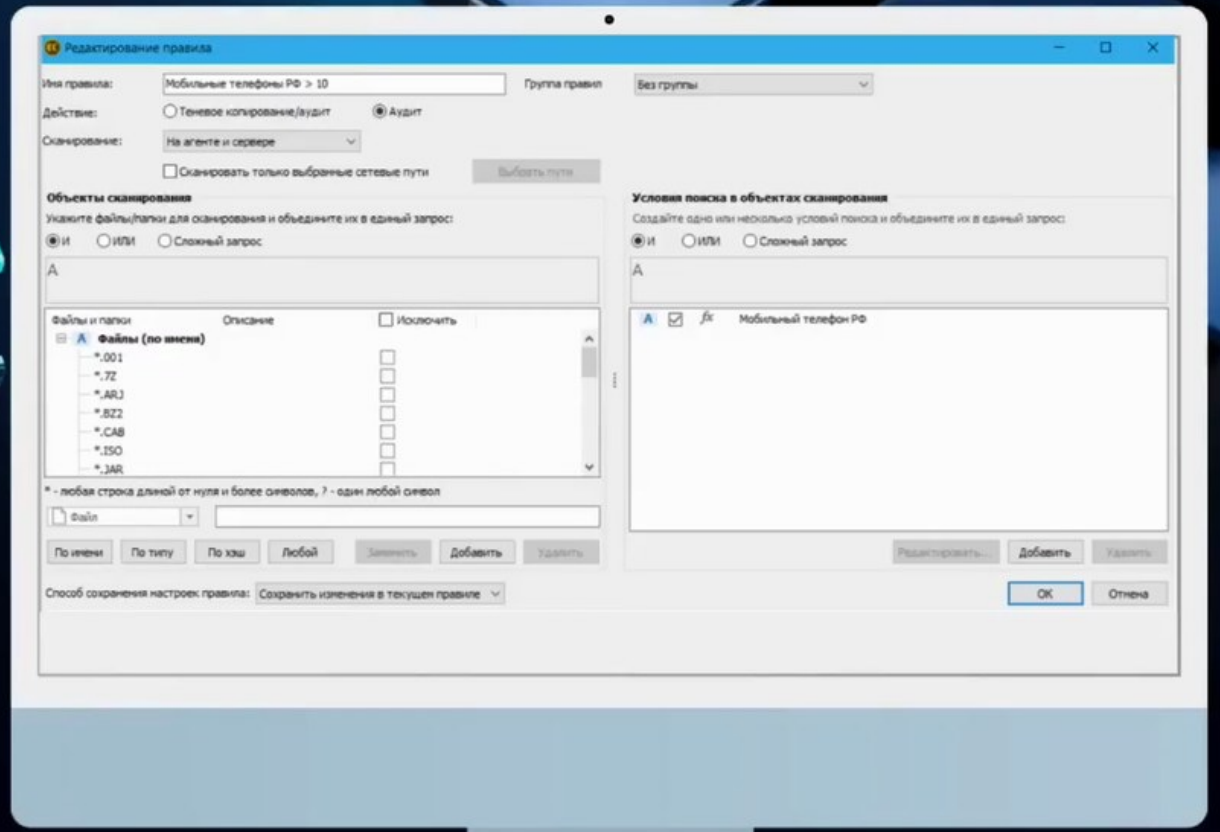
CONCLUSION



Use different steganography methods depending on the data transmission channel and the type of data transmitted.

CONCLUSION

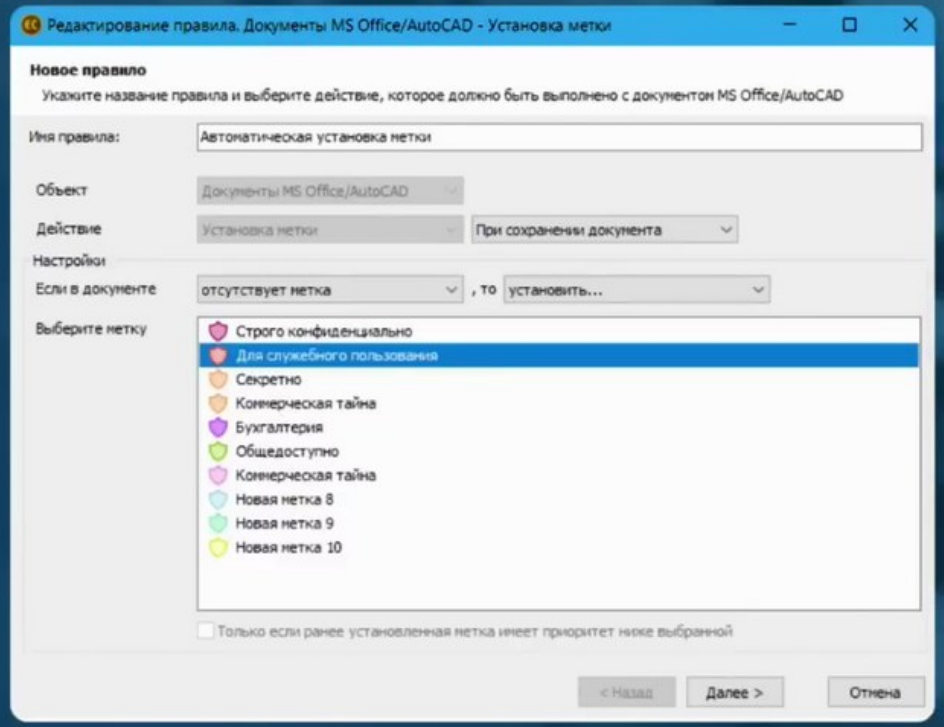
But you can come up with something universal too



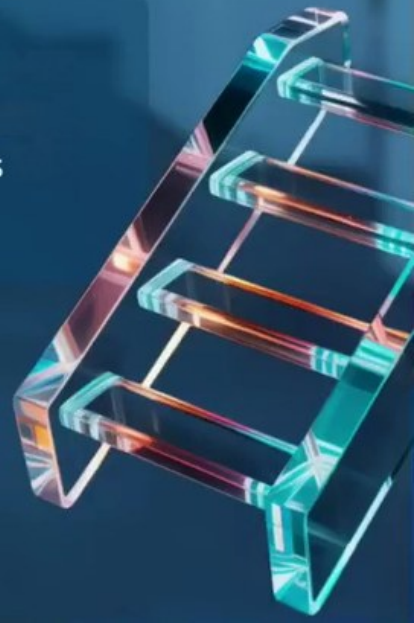
SEARCHINFORM

PROSPECTS

SEARCHINFORM



But you can come up with something more or less universal, moving towards RMS and ABAC



THANK YOU FOR YOUR ATTENTION!

SEARCHINFORM

https://t.me/searchinform

https://vk.com/
securityinform

PRACTICE AND ANALYTICS

https://searchinform.ru/
practice-and-analytics/