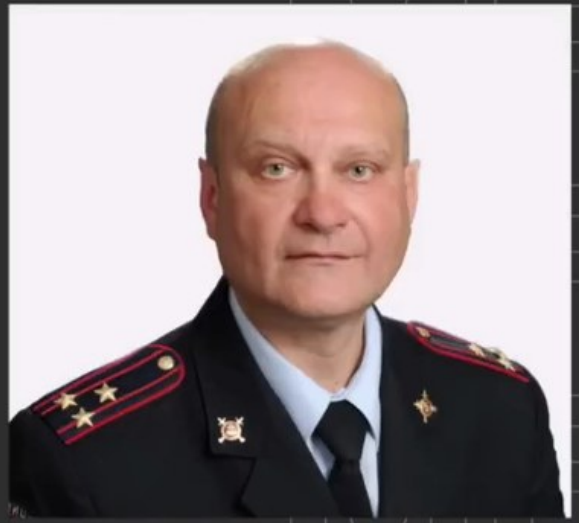
MOSCOW FORENSICS DAY '25

YURI BARKALOV

"HOW DOES OSINT AFFECT INFORMATION SECURITY?"



MFD

How does OSINT affect information security?

Barkalov
Yuri
Mikhailovich



Head of engineering and technical examinations and training.

НАУЧНЫЙ ЦЕНТР
ФОРЕНЗИКА

г. Воронеж, ул. Солнечная 31А,
оф. 440

+7 (473) 280 08 80
+7 (995) 126 70-07
+7 (951) 866 11-38

НАУЧНЫЙ ЦЕНТР
ФОРЕНЗИКА

OSINT (Open-source intelligence) – literal translation: intelligence from open sources. In the Russian security agencies it is Analytical intelligence, though terms such as computer or competitive intelligence also occur.

Collecting information from open sources is all clear!

Main thing – obey the law: Criminal Code Art. 272.1, Art. 152.2 Civil Code

НАУЧНЫЙ ЦЕНТР ФОРЕНЗИКА

Why they collect (-).

Preparing attacks, including on government agencies.

(I got a call, and not just one!)

Blackmail.

- Theft.
- Fraudulent acts.
- …

Why they collect (+).

- Collecting information about employees.

Checking for data leaks.

Investigating crimes.

- Commercial activity.
- ….

НАУЧНЫЙ ЦЕНТР
ФОРЕНЗИКА

Where's the data from!

- We post it ourselves.
- They use leaked data.
- And, oddly enough, open sources, though many of them are paid,

BUT

- Data theft from phones and computers, etc.

НАУЧНЫЙ ЦЕНТР
ФОРЕНЗИКА

BUT! Is this still OSINT in the classic sense!?

Nowadays the method of collecting information is far from passive.

And OSINT is already used by practically everyone providing access to their sites, not to mention the GIANTS of the IT industry!

Including by attackers!

НАУЧНЫЙ ЦЕНТР ФОРЕНЗИКА

Этот сайт осуществляет сбор и обработку файлов cookie, персональных данных посетителей сайта посредством интернет-сервисов веб-аналитики «Яндекс Метрика». Продолжая использовать сайт, вы соглашаетесь на обработку файлов cookie и Политикой конфиденциальности и обработки персональных данных.

OK

License agreement for the use of Yandex Browser software

The user is notified and agrees that the Rights Holder and Yandex.Technologies LLC (119021, Russia, Moscow, Lva Tolstogo St., 16) process their personal data (including but not limited to information about the sites they visited, a trustworthiness rating and/or its derivatives) in order to verify the User's trustworthiness.

Terms of use of the Yandex Metrica and AppMetrica service.

19. Yandex treats all data collected and stored by the Service as the User's personal data and confidential information and, in the cases provided for by applicable law, as the User's trade secret. Unless otherwise provided by applicable law or the Agreement, Yandex undertakes to keep the data secret and not to transfer such data to third parties

НАУЧНЫЙ ЦЕНТР
ФОРЕНЗИКА

TERMS OF THE MICROSOFT CORPORATION SOFTWARE LICENSE AGREEMENT

By accepting the terms of this agreement and using the software, you agree that Microsoft may collect, use and disclose your data in accordance with the Microsoft Privacy Statement

Microsoft Corporation Privacy Statement

Microsoft Corporation collects data obtained from users in the course of interaction with them and our products. Users provide some of this data directly, and some of it Microsoft Corporation obtains by collecting data about interactions with users and their interactions with our products.

AND INFORMATION OBTAINED WHEN ISSUING DISCOUNTS AND CERTIFICATES!

НАУЧНЫЙ ЦЕНТР ФОРЕНЗИКА

Federal Law of ON PERSONAL DATA N 152-FZ

Article 3. Main concepts used in this Federal Law

For the purposes of this Federal Law the following main concepts are used:

1. personal data - any information relating directly or indirectly to an identified or identifiable natural person (the personal data subject.

Article 19. Measures to ensure the security of personal data during processing

1. When processing personal data the operator is obliged to take the necessary legal, organizational and technical measures, or to ensure that they are taken, to protect personal data against unlawful or accidental access to it, destruction, alteration, blocking, copying, provision, dissemination of personal data, and against other unlawful actions in respect of personal data.

GOST R 50922-2006. Information protection. Basic terms and definitions

Information [data] security: The state of protection of information [data] in which its [their] confidentiality, availability and integrity are ensured

2.2.1 legal information protection: Protection of information by legal methods, including the development of legislative and regulatory legal documents (acts) governing the relations of parties in the protection of information, the application of these documents (acts), and also supervision and control over their implementation.

2.2.2 technical information protection; TZI: Protection of information consisting in ensuring, by non-cryptographic methods, the security of information (data) subject to protection in accordance with the applicable law, using technical, software and software-hardware means.

2.3.5 protection of information against disclosure: Protection of information aimed at preventing the unauthorized communication of protected information to interested parties (consumers) that have no right of access to that information.

2.5.2 protected information: Information that is an object of ownership and is subject to protection in accordance with the requirements of legal documents or with requirements established by the owner of the information.

НАУЧНЫЙ ЦЕНТР
ФОРЕНЗИКА

NATURALLY, ALL THIS COLLECTED DATA IS PROTECTED!

??

??????????????????

НАУЧНЫЙ ЦЕНТР
ФОРЕНЗИКА

The main task of OSINT is to sift the truth from unreliable data, analyse it and draw the right conclusions! Analytics!

And it doesn't matter HOW the information was obtained!

From the point of view of science such information has qualitative, quantitative and value characteristics.

For attackers using OSINT to deceive the public at large, apart from the value characteristics of course, this data doesn't matter – they need a phone number and subscriber details!

Then it's all like THE FIELD OF MIRACLES IN THE LAND OF FOOLS from the film The Adventures of Buratino!

"As long as there are fools in this world, living by deception suits us fine!"

But! Unless they're aiming at something big!

НАУЧНЫЙ ЦЕНТР
ФОРЕНЗИКА

Is there any protection?

That's the question.

Follow information security rules!
Anti OSINT - launch disinformation.
(Counterintelligence activity)

Thank you for your attention! Questions?

