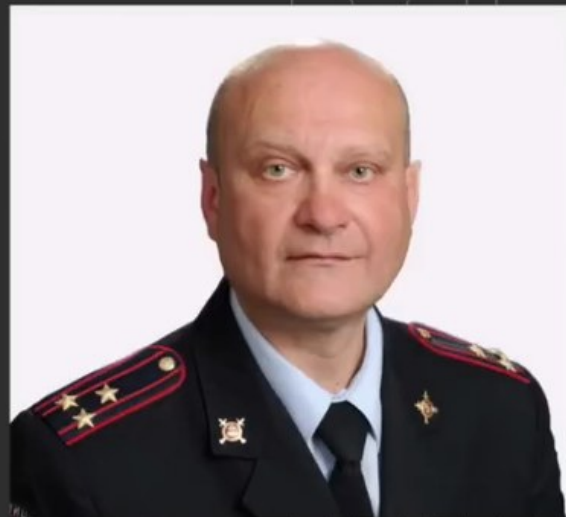


MOSCOW FORENSICS DAY '25

ЮРИЙ БАРКАЛОВ

«КАК OSINT ВЛИЯЕТ НА ИБ?»



Как OSINT влияет на ИБ?

**Баркалов
Юрий
Михайлович**



**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



**Руководитель направления
Инженерно-технических
экспертиз и обучения.**



НАУЧНЫЙ ЦЕНТР
ФОРЕНЗИКА

OSINT (Open-source intelligence) дословный перевод разведка по открытым источникам. В Российских силовых структурах это Аналитическая разведка, хотя встречаются и такие термины как компьютерная или конкурентная разведка.

Со сбором информации в отрытых источника все ясно!
Главное закон соблюдать, УК РФ Статья 272.1. ст. 152.2 ГК РФ

Для чего собирают (-).

- Подготовки атак в том
- числе на Госструктуры.
(Был мне звонок и не один!)
- Шантажа.
- Краж.
- Мошеннических действий.
- ...

Для чего собирают (+).

- Сбор информации о
сотрудниках.
- Проверка утечек данных.
- Расследование
преступлений.
- Коммерческая деятельность.
-

Откуда данные!

- Сами размещаем.
- Пользуются слитыми.
- И, как не странно, открытые источники, правда многие из них платные,

НО

- Кража данных с телефонов и компьютеров и др.



НО! OSINT ли уже это в классическом понимании!?

В настоящее время используется далеко не пассивный метод сбора информации.

И OSINT используется уже практически всеми кто предоставляющими доступ к своим сайтам, не говоря уже о ГИГАНТАХ IT индустрии!

В том числе и злоумышленниками!



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

Лицензионное соглашение на использование программ Яндекс Браузер

Пользователь уведомлен и согласен с тем, что Правообладатель и ООО"Яндекс.Технологии" (119021, Россия, г. Москва, ул. Льва Толстого, дом 16) **обрабатывают его персональные данные** (включая, но не ограничиваясь, информацию о посещенных им сайтах, оценку благонадежности и (или) ее производные) с целью проверки благонадежности Пользователя.

Условия использования сервиса Яндекс Метрика и AppMetrica.

19. Все данные, собираемые и хранимые Сервисом, Яндекс рассматривает как **персональные данные и конфиденциальную информацию** Пользователя, а в случаях, предусмотренных применимым законодательством — как коммерческую тайну Пользователя. Яндекс обязуется, если иное не предусмотрено применимым законодательством или Соглашением, сохранять данные в тайне и не передавать такие данные третьим лицам



НАУЧНЫЙ ЦЕНТР
ФОРЕНЗИКА

УСЛОВИЯ ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ НА ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КОРПОРАЦИИ МАЙКРОСОФТ

Принимая условия настоящего соглашения и используя программное обеспечение, вы соглашаетесь с тем, что Microsoft может собирать, использовать и раскрывать ваши данные в соответствии с Заявлением о конфиденциальности Microsoft

Заявление о конфиденциальности корпорации Майкрософт

Корпорация Майкрософт собирает данные, полученные от пользователей в процессе взаимодействия с ними и нашими продуктами. Пользователи предоставляют некоторые из этих данных напрямую, а часть из них корпорация Майкрософт получает, собирая данные о взаимодействии с пользователями и их взаимодействии с нашими продуктами.

А ИНФОРМАЦИЯ ПОЛУЧАЕМАЯ ПРИ ОФОРМЛЕНИЕ СКИДОК И СЕРТИФИКАТОВ!



Статья 3. Основные понятия, используемые в настоящем Федеральном законе

В целях настоящего Федерального закона используются следующие основные понятия:

1. персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.



Безопасность информации [данных]: Состояние защищенности информации [данных], при котором обеспечены ее [их] **конфиденциальность**, доступность и целостность

2.2.1 правовая защита информации: Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

2.2.2 техническая защита информации; ТЗИ: Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

2.3.5 защита информации от разглашения: Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

2.5.2 защищаемая информация: Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**ЕСТЕСТВЕННО, ВСЕ ЭТИ СОБРАННЫЕ
ДАННЫЕ ЗАЩИЩЕНЫ!**

??

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

Основная задача OSINT отсеять истину от недостоверных данных, проанализировать её и сделать правильные выводы! Аналитика!

И не важно КАК была получена информация!

С точки зрения науки такая информация имеет качественные, количественные и ценностные характеристики.

Для злоумышленников использующих OSINT для обмана населения в широком смысле, кроме разумеется ценностных характеристик, эти данные не важны им нужен номер телефона и данные абонента!

А далее всё как НА ПОЛЕ ЧУДЕС В СТРАНЕ ДУРАКОВ из фильма Приключения Буратино!

«Покуда есть на свете дураки, Обманом жить нам, стало быть, с руки!»

Но! Это если не нацелены на крупное дело!

Есть ли защита?

That's the question.

Соблюдать правила обеспечения ИБ!
Анти OSINT - запустить дезинформацию.
(Контрразведывательная деятельность)

Спасибо за внимание! Вопросы?



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

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

Заказать звонок

Экспертизы ▾

Информационная безопасность ▾

Юридические услуги в сфере IT ▾

Контакты



**Услуги в сфере информационных технологий,
информационной безопасности и судебной
экспертизы**

Подробнее

